Примљено: 23. мај 2023.
Прихваћено: 05. октобар 2023.

УДК 343.982.323:004.451.52.056.5(438)
COBISS.SR-ID 151586057
DOI: 10.5937/ssb2401019G

FACIAL RECOGNITION SYSTEMS FROM THE PERSPECTIVE OF EUROPEAN DATA PROTECTION STANDARDS IN POLAND

Urszula GÓRAL, PhD,
Cardinal Stefan Wyszyński University in Warsaw

FACIAL RECOGNITION SYSTEMS FROM THE PERSPECTIVE OF EUROPEAN DATA PROTECTION STANDARDS IN POLAND

Summary: *In Poland, facial recognition for public security purposes is a matter subject to various legal acts. The aim of the paper is to indicate the legal acts that regulate these issues, the way in which Poland approaches data protection in the context of the use of recognition systems, as well as the way of harmonizing with European guidelines. The paper offers a continuation of the discussion on the need to ensure the security of the state in accordance with the basic rights and freedoms of citizens using this technology.*
Keywords: *face recognition, biometric data, Poland.*

Introduction

A discussion of the use of face recognition systems should be preceded by an explanation of the term FRT. In the most general terms, automatic face recognition (FRT) is a technology that involves the use of an automated mechanism to recognise people based on the analysis of a facial image. The general principle of this type of technology is that algorithms detect a face in an image (photo, recording), then the features of the face (characteristic points, distances between points) are determined, and the next stage is the recognition of the person (or lack of recognition) as a result of comparing the determined features with a master database.

Automatic face recognition is one of the biometric technologies, i.e. mechanisms based on measuring physical (anatomical) features or behavioural (behavioural) analyses of people and comparing them with reference features, allowing for the recognition of individuals. While some mechanisms in this area, such as fingerprint-based identification, considered traditional, have been in use for many years, technological

developments are leading to the emergence of more and more advanced methods of recognising people, based on performing analyses using artificial intelligence and new information processing technologies.

Although automatic face recognition is not the most effective of these methods (iris image analysis is more accurate, for example), face recognition is a technology which as a rule does not require the cooperation of the person being recognised, direct and close contact with such a person is not necessary (capturing the image used for measurement is done from a distance), and the technology (from the technical point of view) is possible to use even without the person's knowledge. It is also worth mentioning biometric applications based on behavioural analysis – information systems are increasingly able to recognise persons not on the basis of their physique, but on the basis of an analysis of their behaviour (e.g. the sound of their voice, the way they walk or the way they type on a computer keyboard).Automatic face recognition can be used to identify a person or to verify a person's identity. Identification of a person involves establishing the identity of the person (identifying the person) by comparing the person's face (data generated by the software based on the facial image) with a pattern stored in a database. Identity verification involves verifying (confirming or denying) a person's identity. Identification of persons based on automatic face recognition generally requires the collection of large databases containing resources to recognise the person, while verification of identity is often performed on the basis of a pattern stored on the user's device (e.g. phone or computer).

Sometimes automatic face recognition is also used to perform other functions, such as emotion recognition, given that facial expressions (facial expressions) can express different emotions (including joy, anger, fear, disgust, indifference, sadness and surprise), or gender, age recognition, etc.

The use of threat recognition systems implies the processing of biometric data within the meaning of the GDPR, the principles set out therein guaranteeing respect for citizens' privacy. As a normative act of the European Union, the GDPR is directly applicable in Poland and is of great importance for the regulation of personal data protection. It defines, inter alia, the principles of personal data processing, the rights of individuals to protect their data and the requirements related to its collection and storage. Consequently, the use of devices that allow for real-time facial recognition raises a number of challenges in terms of ensuring that their use complies with data protection regulations. In particular, whether the technology is

used in accordance with the principles of necessity and proportionality may be of concern, as its use by public authorities is subject to specific rigours set out in the law. Well-established legal standards in the EU require that authorised tools using FRT, must be deployed in a manner fully consistent with what is necessary and proportionate to achieve the objectives and solve the problems they are intended to prevent. Hence, there are many objections to the use of video surveillance systems equipped with relevant functionalities and algorithms that have not been proven and demonstrated to achieve the goal of preventing crime and providing security.

During more than 20 years of combating terrorist attacks and during the coronavirus pandemic, public authorities have significantly stepped up their regulatory activities, leading to a gradual increase in the use of surveillance measures in public spaces.

Polish experience

In Poland, facial recognition for public security purposes is an issue that is subject to various legal acts. The introduction of such technology raises a number of issues related to the protection of privacy, citizens' freedom and control over personal data. Facial recognition, also known as biometric technology, is increasingly popular in the field of public security. In Poland, there are several legal regulations on this issue, which aim to both protect citizens' privacy and ensure public safety.

In the provisions of Polish law, we can find regulations on image processing in the form of facial image fixation by certain services. "Facial image fixation" should be understood, simply, as the taking of photographs (including signature photographs, in accordance with the principles set out in the Regulation of the Minister of Internal Affairs and Administration of 21.07.2016 on information processing by the Police, Journal of Laws, item 1091) of a person in several shots, using the methodology of modern forensic techniques. The ordinance on taking and transmitting fingerprint images and biological material, as well as capturing and transmitting the facial image of a non-citizen also mentions making sketches and verbal descriptions of the images. However, the question arises, unresolved, as to why the law limits the entitlement only to the image of the face and not the head, let alone the entire figure. Especially as both the Police Act and the Border Guard Act do not contain such restrictions on the preservation of the image. This is an unreasonable solution, since it is often the image of the

whole silhouette that may be decisive for personal identification, especially in the case of high similarity between persons.

Key laws and regulations that relate to facial recognition in the context of public safety are discussed below:

The Constitution of the Republic of Poland:

The Constitution guarantees the rights of citizens, including the right to protection of privacy and personal data. Everyone has the right to bodily integrity, as well as to the protection of personal data.

Personal Data Protection Act (PDPA):

This Act regulates the collection, processing and storage of personal data. The controller of personal data must be clearly marked and data may only be collected and processed for specific purposes and in accordance with the law.

Law on the Protection of Critical Infrastructure:

Poland has a law that aims to ensure an adequate level of protection of the country's critical infrastructure, such as telecommunications networks, energy networks, water supply networks, etc. Accordingly, facial recognition can be used to ensure the security of these institutions.

Police Act:

The police in Poland may use facial recognition technology to ensure public safety and law enforcement. However, the use of this technology must be respected within the limits of the regulations and procedures. The police have the right to record demonstrations and their participants, as this power derives from the general provisions of the Police Act – Article 15(1) (5a) of the Act allows officers to observe and record by technical means images of events in public places. The police treat the recording of demonstrations as a standard, procedure-compliant action to ensure security and to gather potential evidence in the event of irregularities or breaches of order. If no violations are found, the collected material is archived and then destroyed in accordance with archiving regulations.

The Act on the Protection of the Name of the Republic of Poland:

This Act sets out the rules and procedures for the use of state symbols, which may affect how and to what extent facial recognition technology is used.

Anti-Terrorism Act:

The provisions of this act regulate issues concerning the fixation of facial image and define the prerequisites authorising the taking of a fingerprint image, the fixation of facial image, the taking of DNA material. Under this Act, officers of the ABW, Police and Border Guard are authorised to take a fingerprint image or record the facial image or non-invasively collect biological material for the purpose of determining the DNA profile of a person who is not a citizen of the Republic of Poland, when:

- there is a doubt as to the identity of the person or
- there is a suspicion of illegal crossing of the border of the Republic of Poland or a concern regarding the declared purpose of stay on the territory of the Republic of Poland, or
- there is a suspicion of an intention to stay illegally on the territory of the Republic of Poland, or
- there is a suspicion of a person's connection with an event of a terrorist nature, or
- a person may have participated in a terrorist training course.

The regulations also set out the rules for the transmission of the recorded image to the Police Commander-in-Chief, by registering it in the National Police Information System (KSIP).

In turn, an organisational unit of the ABW or Border Guard transfers this data to an organisational unit of the Police competent according to the place of collection, which in turn also registers it in the KSIP. However, the Commander-in-Chief of the Police may, after fulfilling certain conditions, by way of a decision give permission for data and information to be recorded in the KSIP by means of telecommunication devices by the ABW or Border Guard directly, without the necessity of transmitting such data and information to the organisational units of the Police."

Code of Criminal Procedure:

Where facial recognition is used in a criminal investigation, the procedure set out in the Code of Criminal Procedure must be followed. The police and other services must act in accordance with human rights requirements and the principles of proportionality and legality.

It is important to understand that facial recognition for public security purposes is highly controversial and requires a balance between the protection of citizens and the need to ensure the safety of the public. The implementation of such technology must be supported by proper procedures and the authorities should act in full respect of human rights

and civil liberties. In addition, Polish law may change in the future to better adapt to changing technologies and public safety challenges.

The case law and the role of the supervisory authority have an important role in relation to the use of facial recognition technology in Poland. A discussion of the role of supervisory authorities, such as the UODO (Polish supervisory authority), in the context of facial recognition specifically addresses the issue of their sovereign powers in relation to monitoring the application of the provisions of the GDPR in the context of regulations being introduced authorising the relevant authorities to use FRT.

In accordance with the sectoral inspection plan for 2018, the DPA inspectors carried out an inspection in local government units with regard to the processing of personal data within the framework of municipal video surveillance, including in the context of excluding the use of facial recognition functionality. As a result of the DPA's inspection, it was found that the cameras operating within the city video surveillance systems covered by the inspection do not have or do not have active functionality of facial recognition or the ability to track a person. In addition, these cameras do not record sound.

Due to the progressive technological developments, the possibilities of law enforcement agencies to prevent and combat crime, which may affect citizens' rights and freedoms, have significantly increased. Their impact on civil rights and freedoms has been widely commented on, as well as the necessity and proportionality of using such measures in a democratic state under the rule of law. In particular, this applies to techniques that involve the use of special categories of data, such as biometric data.

The President of the DPA made use of Article 11(1) of the Act of 14 December 2018 on the protection of personal data processed in connection with preventing and combating crime by requesting, in December 2020, the data protection officers of ten competent authorities to verify the lawfulness of the processing of personal data in connection with the use of solutions using facial recognition technology, i.e. the Police, Border Guard, State Protection Service.

In 2021, The President of the DPA found an infringement by the Centre for Intoxicated Persons of Regulation 2016/679 consisting in the recording and registration of sound (voice) in the monitoring system installed at the Centre, i.e. the processing of personal data in this regard without a legal basis. The DPA imposed an administrative fine of PLN 10,000 (approximately €2,500) on the Centre for Intoxicated Persons.

European data protection institutions' approach towards facial recognition systems

The European Data Protection Board in May 2023 adopted guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement. They provide guidance to EU and national legislators as well as to law enforcement authorities on the implementation and use of facial recognition technology systems. Face recognition tools should only be used by authorities, such as the police, in strict compliance with Directive (EU) 2016/680. The adoption of these Guidelines was preceded by a public consultation, after the comments received the guidelines were updated and further clarifications were added. The guidelines provide guidance to EU and national lawmakers, as well as to law enforcement authorities, on implementing and using facial recognition technology systems. Among others, the guidelines stress that facial recognition tools should only be used in strict compliance with the Law Enforcement Directive (LED).

Moreover, such tools should only be used if necessary and proportionate, as laid down in the Charter of Fundamental Rights.

Overall, the strong stance taken in the Guidelines is extremely important to raise awareness of the deeply negative impact that the use of facial recognition and other biometric technologies can have on fundamental rights.

In the guidelines, the EDPB highlights that the use of facial recognition technology is integral to the processing of significant amounts of personal data, including special categories of data. The face and, more generally, biometric data are permanently and inevitably linked to a person's identity.

As such, the use of facial recognition has a direct or indirect impact on a number of fundamental rights and freedoms enshrined in the Charter of Fundamental Rights of the European Union.

Fundamental rights that may go beyond privacy and data protection, such as human dignity, freedom of movement, freedom of assembly and others.

The guidelines indicate that There are certain uses of facial recognition technology that pose an unacceptably high risk to individuals and the public and as such should be generally prohibited.

In particular, remote biometric identification of individuals in publicly accessible spaces poses a high risk of intrusion into the private lives of individuals and has no place in a democratic society because it inherently involves mass surveillance.

In the same vein, The Board considers AI-supported facial recognition systems categorising individuals on the basis of their biometric data into clusters according to their gender, and political or sexual orientation as incompatible with the Charter.

Furthermore, the EDBP is convinced that the use of facial recognition or similar technologies to infer the emotions of individuals is highly undesirable and should be prohibited, with perhaps a few duly justified exceptions.

In addition, the EDPS considers that the processing of personal data in a law enforcement context, which would be based on the database populated by the collection of personal data on a massive and indiscriminate scale, e.g. by 'scraping' photos and facial images available online, in particular those made available through social networks, would as such not meet the strict necessity requirement under Union law.

The European data protection authorities have also commented on the proposal of the AI Regulation.

The ongoing negotiations of the proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence is being currently very much advanced.

The EDPB and the EDPS pay attention to the following elements:

EDPB and the EDPS call for a general ban on any use of AI for an automated recognition of human features in publicly accessible spaces – such as of faces but also of gait, fingerprints, DNA, voice, keystrokes and other biometric or behavioral signals – in any context

EDPB and EDPS recommend a ban, for both public authorities and private entities, on AI systems categorizing individuals from biometrics (for instance, from face recognition) into clusters according to ethnicity, gender, as well as political or sexual orientation, or other grounds for discrimination prohibited under Article 21 of the Charter.

The guidelines provide practical guidance for public authorities wishing to implement and use an FRT system. They include example scenarios of typical use cases for such systems and a description of key issues such as necessity and proportionality test requirements (Annex III).

In the guidelines, the EDPB reiterates its call for a ban on the use of facial recognition technology in certain cases. In doing so, it considers that it should be prohibited:

- remote biometric identification of persons in public spaces;
- facial recognition systems that categorise persons on the basis of their biometric data into clusters according to ethnicity, gender, political or sexual orientation or other grounds of discrimination;

- facial recognition or similar technologies to draw inferences about the emotional state of an individual;
- the processing of personal data in the context of law enforcement, which would be based on the collection of personal data on a mass scale and in a non-discriminatory manner, e.g. through so-called 'scraping' of photographs and facial images available online.

The release of these guidelines, supplemented by comments and changes that emerged from the public consultation that took place, is a good opportunity to look at the use of FRT systems by both companies and public entities.

The EDPB Guidelines on Facial Recognition Technology are an important tool in the protection of personal data in the EU. Organisations and law enforcement agencies should take them into account and align their practices with the principles of necessity, proportionality and legal compliance. The use of facial recognition technology by companies and public entities should be subject to strict regulation and oversight to prevent abuse and infringement of individuals' rights. There is a need for a balanced approach to the use of facial recognition technology to protect the privacy of individuals and avoid potential discrimination or abuse.

Summary

In Europe, there is a recurring discussion on the use of biometrics for counter-terrorism, crime prevention or public security purposes.

Outlining the above challenges of facial recognition in the context of public security and possible further developments and regulations, this is a further step in the discussion on the need to ensure state security in line with the fundamental rights and freedoms of citizens. Discussing the problems associated with the use of FRT mechanisms requires emphasising the need for a balance between security and privacy and the importance of protecting citizens' privacy and the need to balance this protection with the need to ensure public security.

СИСТЕМИ ПРЕПОЗНАВАЊА ЛИЦА ИЗ ПЕРСПЕКТИВЕ ЕВРОПСКИХ СТАНДАРДА ЗАШТИТЕ ПОДАТАКА У ПОЉСКОЈ

Urszula GÓRAL, PhD,
Cardinal Stefan Wyszyński University in Warsaw

Сажетак

У Пољској, препознавање лица у сврхе јавне безбедности предмет је различитих правних аката. Циљ рада је да укаже на правне акте који регулишу ова питања, начин на који Пољска приступа заштити података у контексту коришћења система препознавања, као и начин усклађивања са европским смерницама. Рад нуди наставак расправе о потреби обезбеђења безбедности државе у складу са основним правима и слободама грађана који користе ову технологију.

Кључне речи: *препознавање лица, биометријски подаци, Пољска.*