Примљено: 10. јун 2023.
Прихваћено: 21. март 2023.

УДК 343.982.323:342.7(497.4)
COBISS.SR-ID 151593737
DOI: 10.5937/ssb2401045L

# FACIAL RECOGNITION TECHNOLOGIES AND HUMAN RIGHTS – A BRIEF COUNTRY REPORT (SLOVENIA)

Rosana LEMUT STRLE, specialist in the field of administrative law, the field of personal data protection and access to public information, CIPP/E, CIPM, Univerza v Ljubljani, Pravna fakulteta

# FACIAL RECOGNITION TECHNOLOGIES AND HUMAN RIGHTS – A BRIEF COUNTRY REPORT (SLOVENIA)

**Summary**: *The paper aims to describe the practice of using facial recognition technology and the impact it has on human rights in Slovenia. For this purpose, a case was used when public suspicion arose that the police were using facial recognition technology to identify participants in anti-government protests. The conclusion reached in the paper is that the Slovenian regulation on the use of automatic facial recognition systems seems proportionate, while some questions such as "is this technology necessary in a democratic society" remain open.*
**Keywords**: *biometric technology, modern society, Slovenia.*

For me, it is fascinating to reflect on the rapid development of our society as today's reality is in many aspects similar to ones from the science fiction films of my childhood. While there is still some room for development on one side (it would be interesting to be able to actually use the phrase "Beam me up, Scotty" from Star tracks in real life), it feels like we are not far from the billboards greeting each customer in the shopping mall and offering them a pair of jeans, perfectly individualised to their preferred style and fit, similarly to the corresponding scene with Tom Cruise in the Minority Report.

Facial recognition technologies are no longer novelties of techno-deterministic elites or mere prototypes. Today, automatic facial recognition technology is widely available on the market.

In Slovenia, it has been possible for a number of years now to buy front doors that can be unlocked by scanning your face. They are advertised with an inviting slogan: "*You come home with your hands full of shopping bags and instead of frantically searching for your key, card, phone or other tool, your front door recognizes you and automatically opens to welcome you as you enter, after which it gently closes itself following your step.*" One of the

wittiest comments on the proposed solution said: "The front door key was first used six thousand years ago, and since 2020 a man has a problem with bags in his hands preventing him from unlocking the door?!" Maybe, it's time to replace the *bags* with something else? This is a thought-provoking illustration of the direction of utilising personal data in the context of "smart homes", notwithstanding the fact that it is out of scope of the GDPR. Note, that the provisions of the GDPR do not apply to the processing of personal data by a natural person in the context of an exclusively personal or domestic activity, without any connection to a professional or commercial activity.

Many of us have already encountered entering a country while traveling by checking an ID document with the simultaneous use of a face reader. Matching the passport photo with the features the device has read on our face allows us to quickly walk through the terminal and enter a foreign country. There is also a strong tendency to introduce automatic facial recognition directly before boarding the plane.

The essential difference between the example of one's front door being unlocked by facial recognition and the use of a face reader to verify a person's identity when entering a foreign country or a plane are the rules that leave room for the individuals and bind the controllers and processors.

The mentioned difference also affects the approach of presenting advantages of the use of biometric technology. When we address an individual, we convince him with arguments about the obsolescence of keys, cards, even of the use of smartphones. We are talking about the comfort brought by automatic face recognition, about the luxurious facilitation of otherwise small but annoying everyday tasks, such as unlocking the front door with your hands full, using different passwords for home electronics, etc. We persuade the individual to move with the times. And he/she can only do this by replacing old, outlived gadgets with the trendy ones – like face scanning front doors.

Whenever data controllers want to justify the use of biometric technology, they usually use the security argument, arguing that this will bring better individual safety and security and public safety. The argument goes that a small rollback of human rights is a reasonable price to pay for greater order and security in society.

And so, we are faced with one of the biggest dilemmas of modern society: Prioritize human rights and freedoms or security? Further questions arise: Are rights and freedoms really curtailed with the greater use of biometric technologies? In which cases is interference with rights

and freedoms justified? Do the benefits of the use of technology outweigh the harm caused by interference with human rights? Is the technology reliable enough to justify intervention? How to act when it turns out that the use of technology led to a wrong result?

These are all questions to which there are no unequivocal answers. Each social environment may respond in a different way. The Social Credit System implemented in China seems like science fiction to Europeans. But is it really so contrasting to our experience? The recent outbreak of the Covid-19 pandemic has shown how fragile human rights are and how quick and effective governmental interventions can be – also in Europe. If the goal (like public health) is presented convincingly and accepted by the public, it quickly justifies even very invasive means for the rights of individuals; a ban on movement, a ban on gathering, increased control over movement and gathering... And with time it seems that the means themselves become the goal...

Of course, in practice, lawyers are mostly devoted to curbing the use of technology by the authorities. Evolution of face recognition systems has inevitably attracted the public sector too, especially law enforcement and border management. This has generated many debates about the impact on human rights. According to Article 8 of European Convention of Human Rights everyone has the right to respect for his private and family life, his home and his correspondence. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

An increasing number of law enforcement agencies in the European Union are using facial recognition technology. Last May, EDPB (European Data Protection Board) recognized this fact in the Guidelines nr. 05/2022 on the use of facial recognition technology in the area of law enforcement.[1] Facial recognition technology may be used to authenticate or to identify a person and can be applied on videos or photographs. It can be used for a variety of purposes, such as searching for people on police watch lists or monitoring a person's movements in public places. It can be used in controlled 1:1 situations, but also in large crowds and major transport hubs. It relies on the processing of biometric data, and therefore involves

[1] Guidelines are published at: https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf

the processing of special categories of personal data as defined by the GDPR. Often, facial recognition technology uses components of artificial intelligence or machine learning.

If a member state of the Council of Europe wants to use facial recognition technology, the prescribed regulation must comply with Article 8 of the European Convention on Human Rights. Additionally, when it comes to a member of the European Union, the compliance with the rules on processing of special types of personal data – biometric data, as defined by the GDPR or possibly the Law Enforcement Directive[2] – must be ensured.

The Slovenian police have been using facial recognition technology since 2014. Not much was known about the legal basis and scope of its use until 2021, when public suspicion arose that the police were using facial recognition technology to identify participants in anti-government protests. It was the time of the pandemic, the right of association was limited to a handful of people (maximum 10), and there was growing dissatisfaction with the government's approach to the pandemic (as well as other aspects of governance). Eventually, the dissatisfaction reached its peak and protests became a constant. Every Friday, people gathered and protested in front of the parliament building. In order to avoid accusations of illegal assembly (a violation of the government's decree on the maximum number of people allowed in one place), the demonstrators cycled around the parliament. Well, if such ingenuity is on the side of the common man, authority, and with it the power to react, is on the side of the government.

At the beginning of 2021, the Information Commissioner received some information and reports with the suspicion that the police had used the automatic facial recognition system to identify the participants of various protest rallies and, after identification, had sanctioned them in misdemeanour proceedings. The Information Commissioner therefore carried out an inspection, which did not reveal any irregularities in the use of the automatic facial recognition system by the Slovenian police.

The legal basis for use of the automatic facial recognition system was introduced with the amendments of the Police Tasks And Powers Act[3] (ZNPPol-A, February 2017). The relevant Article 112, paragraph I reads:

---

[2] Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

[3] Police Tasks And Powers Act (Zakon o nalogah in pooblastilih policije (Uradni list RS, št. 15/13, 23/15 – popr., 10/17, 46/19 – odl. US, 47/19 in 153/21 – odl. US; ZNPPol).

> *In the performance of police tasks, police officers shall collect and process personal and other data, including biometric data and data arising from confidential relationships or professional secrets. Police officers may process data during the identification procedure and in the detection and investigation of criminal offences. In the detection and investigation of criminal offences police officers may, if necessary and required given the circumstances of a concrete criminal offence, compare fingerand palm prints, photographs with photographs of other persons and compare DNA profiles. These data may be processed in an automated manner.*

The Information Commissioner has always opposed the amendment to the ZNPPol, which allowed the use of automated facial recognition. In the period from 2015 to 2019, it issued seven negative opinions[4] regarding the provisions of the ZNPPol, which regulate the processing of biometric data. The IC's comments emphasized the need for a data protection impact assessment before the adoption of the legislation. It also pointed out that the police is not authorised to control "all public resources" in general, especially not posts on social networks, forums and similar sites with user-generated content. For example, the Police is not entitled to collect photographs that have been published online by individuals themselves or that have been published about individuals by others. IC highlighted the potentially unacceptable extension of police powers, known as public surveillance. Historically, public surveillance was limited to the decisions of police station commanders to organise observation of riskier places where a higher number of crimes or acts against public order and peace had been recorded. However, it is not permissible to extend the powers of public surveillance to the organisation of public surveillance of all public places, 24 hours a day, every day of the year, with the help of technological tools such as video surveillance and automatic facial recognition. Such a constantly present, non-selective, systematic mass surveillance, without the required justification in the indications of prohibited conduct or reasons for suspecting the commission of a criminal act, is characteristic of the so-called police state and is unacceptable in a democratic society that respects human rights. In its opinions, the Information Commissioner drew on the decisions of the Court of Human Rights in the case of *Zakharov v. Russia*[5]

---

4 Opinion nr. 007-67/2015 from 1.9.2015, opinion nr. 007-10/2016/2 from 8.3.2016, opinion nr. 007-31/2016/3 from 12.5.2016, opinion nr. 007-57/2016/2 from 14.7.2016, opinion nr. 007-51/2018/2 from 29.11.2018 and opinion nr. 007-51/2018 from 11.1.2019.

5 ECHR Application no. 47143/06; judgement from 4 December 2015.

and *Szabo and Vissy v. Hungary*[6], as well as on the decision of the Court of Justice of the European Union in the case of *Digital Rights Ireland*[7].

After the adoption of amendments to the ZNPPol in 2017, the Information Commissioner, that only has limited authorities to request an assessment before the Constitutional Court of the Republic of Slovenia, proposed to the Ombudsman to submit a request for a review of the constitutionality of the new Article 112, paragraph I of the ZNPPol.

The Ombudsman, however, did not challenge the use of automatic facial recognition technology before the Constitutional Court. When asked why not, he replied that the Information Commissioner itself had already assessed in his observations that civil society had not expressed serious objections to the use of facial recognition technology by the police. This circumstance therefore led to the Ombudsman's conclusion that the use of facial recognition technology, as legislated in the ZNPPol, is recognized as acceptable in Slovenian society.

In addition to the provision of Article 112, the ZNPPol also includes a safeguard in Article 122, which regulates Automated processing of personal and other data.

The police must not use any automated processing of personal or other data (processing of personal or other data by means of information technology) that could result in a decision being adopted, motion or criminal complaint being filed or report being drawn up concerning a natural or legal person or other entity that could, if no further action or decision was taken by a competent police employee, prejudice the rights or obligations of the natural or legal person or other entity. The police must not make personality profiles of persons to whom personal data refer through automated processing of personal or other data, in particular the aggregation or comparison of personal data from one or more personal data filing systems, records, public or other registers or other data bases containing personal data, so that it could be concluded, if no action or decision was made by the competent police employee, that the persons concerned have committed or have not committed a certain criminal offence or that the testimony of a certain person is reliable or not. The use of automated processing of sensitive personal data to make a personality profile of a person shall be prohibited.

In the inspection procedure, which ended in april 2021, the Information Commissioner found that the system used by the Slovenian police (Face

[6] ECHR Application no. 37138/14; judgement from 12 January 2016.

[7] Joined Cases C-293/12 and C-594/12; judgement of Grand Chamber from 8 April 2014.

Trace) is based on biometric processing of personal data, but does not enable identification (like the Clearview system, for example). It only enables comparison by similarity to the described perpetrator and it only works within the police information system.

For the purpose of automatic face recognition, the Slovenian police uses photographs of the faces of individuals, which are processed in the police Record of Photographed Persons[8] – i.e. the faces of suspects of criminal offenses photographed by the police on the basis of Article 149/II of the Criminal Procedure Act[9]. In the comparison process, the police process photos from Evidence in the Face Trace module, which is an automated way of processing biometric data. According to the first paragraph of Article 112 of the ZNPPol, this method of processing personal data is permissible only in the detection and investigation of criminal acts, when it is necessary in view of the circumstances of the commission of a specific criminal act.

The recognition process in the Face Trace module takes place in such a way that a photo robot or a recording of a suspected criminal (for example, made from a video surveillance system) is entered into the Record as a picture of an unknown person, the module than performs an automatic comparison with photographs of persons from the Record.

The result of this comparison is a list of persons classified according to their similarity to the described offender. The final identification of a person is always done "manually" by an expert of comparison of facial features.

According to the police, the process of automated photo comparison can only be carried out within the police system. In the inspection procedure, the Information Commissioner did not establish that the Face Trace module could be used in a way that would allow a direct comparison of photos located on the Internet or elsewhere outside the police system with photos from the Record. The police must therefore always enter (import) the photo they want to compare with the photos from the Record into their information system, where they can then perform a comparison using the module for automated face recognition. The police denied the use of the Clearview application and the Information Commissioner did not establish its use in the procedure.

---

8 The Record contain the following elements: "Nickname or false name, photograph, personal description, place, time and reason of photographing, personal name of the person who took the photograph.

9 Zakon o kazenskem postopku – Criminal Procedure Act (Official Gazette RS, nr. 176/21 – official consolidated text, 96/22 – judgement of Constitutional Court and 2/23 – judgement of Constitutional Court).

The police also claim that they use automated facial recognition (the Face Trace module) only in the detection and investigation of crimes, but not in the performance of other police duties. In the process, the Information Commissioner did not come across any indications that would show otherwise.

After the inspection, the Information Commissioner in a public statement added that, in practice, the system for automatic facial recognition could be used for purposes that are not permitted by law. However that the police also have system of safeguards in place, which on the one hand reduce the possibility of abuse, and on the other hand enable their subsequent identification. The police has a properly established system of providing an audit trail of personal data processing with the Face Trace module, which enables subsequent verification of the legality of personal data processing.

In my opinion, the Slovenian regulation of the use of the system for automatic face recognition (the Face Trace module was produced and maintained by a Slovenian company) appears to be proportionate. Whether it is necessary in a democratic society is a question that remains open. So far, neither the Ombudsman nor the Information Commissioner has recognized its use as an inadmissible interference with human rights. In addition to the balance of the use itself, control is also important. It can only be effective if traces of system usage are reliably recorded. The Information Commissioner assessed that the recording of the use of the Face Trace module is adequate, which installs trust in the observance of statutory restrictions.

# ТЕХНОЛОГИЈЕ ПРЕПОЗНАВАЊА ЛИЦА И ЉУДСКА ПРАВА – КРАТАК ИЗВЕШТАЈ ДРЖАВЕ (СЛОВЕНИЈА)

Rosana LEMUT STRLE, specialist in the field of administrative law,
*the field of personal data protection and access to public information, CIPP/E, CIPM, Univerza v Ljubljani, Pravna fakulteta*

***Сажетак***

Рад има за циљ да опише праксу коришћења технологије препознавања лица и утицај који она има на људска права у Словенији. У ту сврху је коришћен случај када се појавила сумња у јавности да полиција користи технологију препознавања лица како би идентификовала учеснике антивладиних протеста. Закључак до којег се дошло у раду јесте да се словеначка уредба о употреби система за аутоматско препознавање лица чини пропорционалном, док нека питања, попут „да ли је ова технологија неопходна у демократском друштву", остају отворена.

**Кључне речи**: *биометријска технологија, савремено друштво, Словенија.*