Примљено: 15. мај 2023.
Прихваћено: 21. септембар 2023.

УДК 343.982.323
COBISS.SR-ID 151328265
DOI: 10.5937/ssb2401011K

THE USE OF FACIAL RECOGNITION TECHNOLOGIES

Urmas KUKK, attorney-at-law,
CIPP/E, KPMG Law Estonia

THE USE OF FACIAL RECOGNITION TECHNOLOGIES

Summary: *The paper discusses the use of facial recognition technology in the Republic of Estonia both by state authorities and in the private sector. The possibility of using facial recognition technology in elections is pointed out, while underlining all the shortcomings that arise in connection with it. Finally, the possibility of using face recognition technology in real time with video surveillance in public space is considered.*
Keywords: *facial recognition, Republic of Estonia, surveillance society*.

Identification based on a person's face is probably one of the oldest methods of identifying a person. Initially, it did not even require an image of a person's face. It was enough for someone who had previously known the person to point the finger at him, and everyone else believed him. With the emergence and spread of literacy, the presence of a person who knew the person was also no longer necessary to identify him. The description of the person also helped. It would be good if the description were as detailed as possible. It was not enough that the person had a nose in the middle of the face. A better description would have been to describe where the nose was slanted or whether the eyes were at the same height. As the skill of portraiture developed, it became possible to transmit the image as reference material, which did not guarantee a flawless identification of identity. The similarity of the reference material (portrait) with the depicted one often depended on the skills and experience of the recorder (portraitist). Furthermore, there is a legend that Henry VIII once had a difficulty identifying the identity of one of his later wives when he compared the person who arrived to him with a portrait sent to him earlier. It is not plausible that Hans Holbein the Younger, who painted the picture, needed more skill or experience. Rather,

he added a good dose of his subjective understanding of what a beautiful woman should look like in the painting.

Be that as it may, to this day, comparing an image with a person remains the most common means of identifying identity. Various methods have come to the aid of the identifier over time. The purpose of all of these is that the ultimately subjective judgment made by the identifier should be as objective as possible. Today, various tools have been added to implement the methods. Still, so that the decision can be made quickly, and the result is as objective as possible. One such tool is facial recognition systems that use different combinations of hardware and software.

Considering the history of the Republic of Estonia, one might think that we have strictly limited activities of law enforcement agencies in monitoring people and their employees refrain from actions that, in the smallest degree, may infringe on a person's rights and freedoms more than what is allowed by legal norms. However, the reality is quite different. Given the country's small size (both in terms of territory and population), we rather observe and follow what is happening elsewhere than proactively discuss important issues. This is for the simple reason that there is still no direct need and no possibility to compare. To compare different personal identification systems using anthropometry in real-time.

The same goes for real-time facial recognition. In Estonia, there has yet to be any public discussion on the necessity of implementing facial recognition technologies and the associated risks and benefits. Probably because the need for real-time facial recognition has not yet arisen. So far, at least, not a single case has reached the public in which the law enforcement bodies claimed that the case would have been solved or solved differently if there had been rapid real-time identification of a person using a facial recognition tool connected to a video camera in a public space.

Compared to law enforcement, facial recognition is used much more in private relationships. And even there, it is only used for one-time identification of the person so that the person can enter the service provider's online environment. However, more than facial recognition is needed to give orders in the online environment. As a rule, additional personal identification means must be used to confirm the order. The use of facial recognition in private relationships must also comply with GDPR requirements.

The activities of law enforcement bodies in processing personal data must meet the requirements set out in Chapter 4 of the Personal Data Protection

Act.[1] This chapter adopted Directive 2016/680.[2] For law enforcement purposes, real-time facial recognition is used today at border crossings. It is also possible within the framework of criminal proceedings, in accordance with Chapter 3[1] of the Code of Criminal Procedure [3] and in the case of surveillance operations, in accordance with §12 of the Security Authorities Act [4]. The law enforcement body does not have to explain exactly how facial recognition takes place in the case of these activities because according to §35 (1) 5[1] of the Public Information Act [5]: "- information concerning the methods and tactics utilized by an investigative body in its activities, if the disclosure of such information could hinder detection of criminal offences or facilitate committing thereof", such information must be declared for internal use of the institution.

The possibility of using facial recognition in elections has been studied in Estonia. Facial recognition has been considered to be implemented in e-elections, not in elections that are conducted in polling stations. The corresponding study was conducted in 2021 [6]. As a result of the study, it was found that facial recognition in the context of e-elections would be very complicated, so initially, this topic has not been elaborated further.

As a result of the study, it was concluded that the application of facial recognition in e-elections leads to new problems, of which the following are likely to arise in real-time facial recognition:

> "– The error rate of facial recognition will never be zero because biometrics-based authentication is a heuristic process. The amount of both false positive and false negative detections depends on the threshold set for identifying a person. If the proportion of false positives of the best currently available solutions is reduced to less than 1 per 100,000, then the number of false negatives would remain at 3% in the case of images taken in home conditions (poor light, arbitrary background, low-resolution camera). This means that, for example, out of 250,000 people, about 7,500 people would be unable to vote.
>
> – Adding facial recognition to the Estonian e-voting protocol would require both making the protocol more complex and introducing additional hardware. This means the protocol becomes more error-prone while degrading the user experience." [7]

---

1 Personal Data Protection Act – Riigi Teataja.
2 EUR-Lex – 32016L0680 – EN – EUR-Lex (europa.eu).
3 Code of Criminal Procedure – Riigi Teataja.
4 Security Authorities Act – Riigi Teataja.
5 Public Information Act – Riigi Teataja.
6 Biomeetrilise näotuvastusmeetme rakendamine e-hääletamisel.pdf (valimised.ee) (Estonian only).
7 Ibid., page 7.

As a rule, voting is a relatively short-term activity; in this case, the person usually does not rush around the room simultaneously. However, there is no guarantee that the voting will be done by the same person from start to finish. Using a video image for real-time facial recognition will probably be even more difficult, because the person to be recognized is presumably not standing still and is most likely not looking at the camera at the same time.

Facial recognition errors during voting are very problematic, but a person can still fulfil his civic duty by using other means of authentication. Certainly, a bigger problem is when an innocent person is detained in the case of a false positive result or the culprit is not arrested in the case of a false negative result of facial reconigation.

Real-time automatic identification, including facial recognition, requires extensive consideration before being deployed by law enforcement agencies.

We can discuss at length whether the surveillance society is a reality or whether we are just on our way there. There is not complete clarity even in what we understand by surveillance society. Is it a society where monitoring of everyone is possible due to the level of development of information technology tools, but their use takes place only in accordance with legal regulations? Or is it a society where surveillance of everyone is possible, but state bodies are not bound by legal norms in their use?

Since data sets covering all persons are not used as a reference base, we have yet to reach a society of total surveillance. I assume…

The use of video surveillance alone has not created the need to rename society a surveillance society. The tracking and recording of its results took place before the person could be depicted in such a way that the viewer would later recognize the person from the image. Photography created the technological possibility for the rapid recording of a (human) image and the telegraph for the fast transmission of that recording. The natural continuation of all this has been the recording and transmission of moving images. Today's information technology makes it possible to process large (huge compared to the time when the telegraph was introduced) volumes of data incomparably faster than twenty years ago. At the same time, the possibility of mistakes has not been reduced to zero. A facial recognition system is only as accurate as the person who created it has been able to make it. However, AI today is only the transmission of statistical results without numerical data. And self-learning with it is nothing more than changing its statistics according to the added data. What data to add, however, is decided by the creator of the system, i.e. the person.

It is essential to determine whether the obtained data can be used and, more importantly, whether it can be used at the right time. Not to mention the competence and authorization of the user when using the data.

Many factors must be considered before deciding whether to implement real-time facial recognition alongside video surveillance in a public space. For example:

1. Why use facial recognition out of all possible anthropometric measurements? Just wearing glasses and/or a face mask is enough to confuse.
2. What is the reference base? Should the reference base only consist of photographs of wanted persons, or persons suspected of serious crimes, or anyone suspected of anything?

For me, the most important issue is how to ensure that law enforcement agencies adhere to all established rules. Whether we call the environment in which we live a surveillance society or a democratic society, it does not provide any guarantee that all the rights and freedoms of all persons in the country are guaranteed. Not even by those institutions that are called and set to protect rights and freedoms from being violated. Law enforcement bodies sometimes tend to interpret the legal norm "creatively". This is for a very humane reason – the facts do not support the gut feeling, but the gut feeling can't be wrong. Therefore, the legal norm can sometimes be interpreted so that gut feelings can be the basis for decision-making.

It is important that the greater the threat to a person's rights and freedoms, the more detailed the use of monitoring and identification means must be regulated. Especially for those who use these tools from a position of power. For example, law enforcement agencies.

However, the biggest problem is that since the decision made by the device may not be 100% true, someone should review the findings and make the final decision.

But are we 100% sure that the outcome of a particular human decision-maker is always objectively correct…

УПОТРЕБА ТЕХНОЛОГИЈА ПРЕПОЗНАВАЊА ЛИЦА

Urmas KUKK, attorney-at-law,
CIPP/E, KPMG Law Estonia

Сажетак

У раду се разматра употреба технологије препознавања лица у Републици Естонији, како од стране државних органа тако и у приватном сектору. Указано је на могућност коришћења технологије препознавања лица на изборима, уз подвлачење свих недостатака који се у вези са тим јављају. Коначно, разматра се могућност коришћења технологије препознавања лица у реалном времену уз видео надзор у јавном простору.

Кључне речи: *препознавање лица, Република Естонија, друштво за надзор*.