FACIAL RECOGNITION

European Forum for Urban Security

CCI
CUTTING CRIME IMPACT

Facial recognition is arguably one of the most polemic and yet ubiquitous applications of AI based computer vision algorithms. It is biometric technology – a process that allows to recognize a person by a physical or behavioural characteristic. Other examples of this are fingerprint or iris recognition, voice recognition but also identification based on gait. Facial recognition comprises two phases. In a first phase, biometric information from the image is used to create a model of the face, which is then, in a second phase, compared to a database of images.[1]

Facial recognition has two functions: The authentication and the identification of a person. In the first case, the system compares the biometric template of a face to a single image of a particular person in order to verify whether or not it is the same person. In the second case, the model is compared to a larger database of pictures in order to identify one person amongst many. A third, highly controversial, function is concerned with categorisation – the differentiation of people into various categories, depending on individual characteristics. Such characteristics commonly include sex, age and ethnic origin.[2] Live facial recognition technology refers to the real-time comparison between recorded footage and images in databases.

[1] Reconnaissance faciale : pour un débat à la hauteur des enjeux. CNIL; 2019. Available from: https://www.cnil.fr/sites/default/files/atoms/files/facial-recognition.pdf

[2] Facial recognition technology: Fundamental rights considerations in the context of law enforcement. European Agency for Fundamental Rights (FRA); 2019. Available from: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper.pdf

FACIAL RECOGNITION IN EVERYDAY LIFE

Facial recognition is a software functionality that can be integrated into a whole panoply of existing technologies and connected to other functionalities. Some smartphones use facial recognition as a security measure that allows only the owner to unlock the phone. If users agree, social media platforms such as Facebook create a template of their face based on tagged pictures and use this to recognise them in photos or videos.

Governments can use the technology to facilitate the provision of online public services. When a user signs up for the French governmental mobile application ALICEM, the app authenticates the provided identification paper through a facial recognition software. Once this authentication process is completed, the user can access public services through the application. In Europe, most experimentation with facial recognition technology happens in the domain of transport. Italy has used the technology to measure the flow of passengers at Rome's Fiumicino airport and a number of French airports, including Charles de Gaulle, have installed the automated passport verification system "Parafe" ("Passage automatisé rapide aux frontières extérieures").

FACIAL RECOGNITION IN URBAN SECURITY AND ITS IMPACT ON THE PERCEPTION OF SECURITY

In the realm of urban security, facial recognition softwares can be used for the prevention, detection and investigation of crime. Examples of applications commonly include support in the search for missing people, in particular children or elderly persons, and the identification and tracking of criminals. Another example is the use of facial recognition to uncover identity theft.

A number of European cities have experimented with facial recognition technology in public spaces. During the 2019 Nice carnival, the city hall and the municipal police tested a facial recognition system in one area of the festival grounds. The London Metropolitan Police Service conducted a number of trials throughout the city, including during the Notting Hill carnival.

The European Cutting Crime Impact (CCI) project focuses part of its research on the measurement and mitigation of feelings of insecurity and crime prevention through urban design and planning (CP-UDP). One issue is that satisfying one group of population may result in excluding another. AI-based surveillance technologies might satisfy some people and improve their perception of security but other groups might perceive them as a sign of unwelcome surveillance in certain public spaces, or that they infringe on individual freedoms. The research also found that increased surveillance might have a similar effect as walls or barbed wire, which have shown to increase feelings of insecurity.[3]

The presence of security cameras and the knowledge that they are outfitted with facial recognition software can thus impact inhabitants' perception of security and even the way they behave in, or use public spaces. Some people might feel uncomfortable using public spaces they know to be under surveillance. This can have negative effects on the freedom of expression and of assembly. Additionally, a limited use of a public space can have economic impacts on the whole neighbourhood.

[3] Davey and Wootton (2019), PIM Toolkit 4: Report on feelings of insecurity - Concepts and models adapted from Davey, C.L., & Wootton, A.B. (2014) "Crime and the Urban Environment: The Implications for Wellbeing", in Wellbeing. A Complete Reference Guide (Eds) Burton, R., Davies-Cooper,R. and Cooper, C. Wiley-Blackwell: Chichester (UK)

LEGAL, SOCIAL AND ETHICAL IMPLICATIONS

Facial recognition technology is controversial for many reasons. Commonly discussed issues concerning the right to privacy, the right to data protection and the right to non-discriminanation are complemented by a larger set of fundamental rights. These must be taken into account to different extents at different points in the process of developing, deploying and evaluating facial recognition software.

1. Fundamental rights

The first fundamental right to take into account is human dignity, which is the foundation of other fundamental rights protected by EU Law. As seen above, the presence of facial recognition technology can impact the way people are using public spaces. This relates directly to the freedom of assembly and of associations, as well as the freedom of expression. Other fundamental rights that need to be taken into consideration when a city decides to experiment with or implement facial recognition technology are: the rights of the child and of older persons, the right to good administration and the right to an effective remedy and a fair trial. Children are particularly vulnerable and the use of their biometric data, including facial pictures, should be accompanied by careful considerations of necessity and proportionality.

Young children's facial characteristics evolve as they grow up, which increases the risk of misidentifications. This applies also to older people, whose facial appearance changes with age and might impact the accuracy of facial recognition. In 2019, the Swedish data protection agency issued its first fine in reaction to a school that tested facial recognition to monitor student's attendance in one class. This experimentation was in violation of a number of General Data Protection Regulation (GDPR) articles.

---

2. Data collection and non-discrimination

While the accuracy of facial recognition technology has improved over the years due to developments in computational power and artificial intelligence, and growing amounts of data, risks of wrong or misidentifications persist. Studies have found that the error rate varies depending on gender and skin colour.[4] Different genders and ethnic origins are not inherently harder to recognise but systems often don't have representative datasets to learn from. Another problem is related to the fact that there is not a lot of research on how facial recognition works for people with disabilities. Such evidence debunks the common assumption that technology is neutral or objective and reinforces the importance of considering the fundamental right to non-discrimination. Measures to prevent bias reproduction and misidentification issues are particularly important during the development phase of the technology.

[4] The Best Algorithms Struggle to Recognize Black Faces Equally, Tom Simonite. Wired, 2019. Available from: https://www.wired.com/story/best-algorithms-struggle-recognize-black-faces-equally/

3. Origin of the data and the software

Since the data used to feed and train the facial recognition software is at the basis of the latter's quality, it is important to understand where it comes from and who collected it for what purpose. It is possible that secondary data is used and in that case, it must be taken into account that the purpose of the data collection is different from the purpose of its current use. Depending on the type of artificial intelligence algorithm used, it is easier or harder to verify where the data is coming from and how the algorithm formed its decisions. A rule-based algorithm is trained by a human-crafted set of rules, which makes verification and evaluation easier. If the algorithm is based on deep learning it necessitates larger quantities of data and generates outputs based on probabilities. This makes the process harder to trace and thus less transparent.

4. Privacy and Data protection

While many European cities and regions are interested in employing facial recognition systems, the question remains whether they have the expertise and resources to ensure that potentially discriminatory consequences are prevented. Not every local authority has the ability to develop a software in-house and to train its law enforcement to work with it. This can reduce transparency and negatively impact the right to good administration, which includes an individual's right to access their file in case and ask for evidence of why a measure against them has been taken (FRA, 2019).

In addition, local authorities must also be able to protect the data from malevolent acts. Breaches might lead to the misuse of the stored personal information of the people whose faces are included in databases used to train the algorithms. Additionally, authorities must be equipped to identify instances in which the algorithm is being tricked. Facial recognition systems can for example be tricked by fake images, a process called "spoofing" in which perpetrators use someone's photo to gain access to personal data.

LOCAL PRACTICES

City of Nice (FR)

In 2019, the city of Nice decided to test live facial recognition during its 135th annual carnival and assess how well the technology worked. The key objectives were to contribute to the securitisation of the public space and support scientific research in order to foster technological advance.

Forty volunteers signed up for their picture to be added in the database against which to compare their images. The experimentation was supported by the monegasque company Confidentia and based on the Israeli Anyvision software. The software can take into account aging, thus recognizing a person up to twenty years after the photograph was taken.

Three scenarios were put in place: controlled access at the entrance gate through face identification, the detection of a person of interest in the crowd, and finding a person of interest when passing through the gates. Participation in this pilot project was voluntary and people visiting the Carnival could choose whether or not to enter the area where the cameras were deployed. In total, 5,000 people ended up participating in the experiment that unfolded over three days.

London Metropolitan Police (UK)

Between 2016 and 2019, the London Metropolitan Police Service (MPS) conducted 10 Live Facial Recognition (LFR) tests in different scenarios and with different watchlists of persons of interest throughout the city. The purpose of these trials were to "assess the value, viability and challenges (including technological, legal, ethical, and governance)" of the technology. The facial recognition software was integrated into cameras that would generate alerts, which officers could then assess and adjudicate.

The MPS used a watchlist of individuals of interest and their facial images as a database, which eventually included 2,401 subjects. Over the three years of testing, LFR was deployed during a total of 69 hours. With approximately 180,000 opportunities of recognition (faces that appeared in the videos), the police engaged with 27 individuals and arrested 9 in response to alerts by the facial recognition system.

The efficiency of the LFR system greatly depends on the number of individuals listed in the watchlist. The increase of the list's size is believed to have contributed to a higher number of identifications and arrests during the second half of the trials. Compared to the "manhunt" tactic where offenders are located by deploying officers to multiple locations over long periods of time, LFR requires less resources and can increase operational efficiency. In terms of location of the cameras, the system was most efficient when there was a level of control over the flow of people passing through the area. They found that while the rate of false positive identifications was statistically insignificant when it came to ethnicity, it was significant in terms of gender difference. Women had both lower false positive identification rates and lower true positive identification rates.

[5] For a detailed description of the experimentation, please see: https://www.met.police.uk/SysSiteAssets/media/downloads/central/advice/met/facial-recognition/met-evaluation-report.pdf
[6] Ibid, page 3.

WHAT CHALLENGES FOR CITIES?

At the operational level, cities can encounter problems due to the complexity of the technology and the novelty of the tool. Without appropriate training, it is difficult to understand how the technology works and how it can be used most effectively. A lack of consideration of the impacts of facial recognition on fundamental rights impacts the legitimacy of its use and can have discriminatory consequences.

Given the complexity of the technology and the ubiquity of its potential uses it becomes crucial to consider how to ensure the protection of fundamental rights and freedoms while responding to security needs. How can anonymity be preserved in the public space? What forms of surveillance are acceptable without raising fears in society and negatively influencing individuals' feelings of insecurity and unsafety?

Considerations when developing and deploying facial recognition technologies

- Working towards a clear legal and regulatory framework: Considering the speed and complexity of new developments in facial recognition technology, the European Union is planning on re-assessing existing legal frameworks, such as the GDPR, and considering new legal requirements. In its white paper on artificial intelligence, the Commission outlines aspects that these requirements are linked to: training data, keeping of records and data, information to be provided, robustness and accuracy, and human oversight. Sharing local experiences, problems encountered and lessons learned on a European level can help anchor such requirements in the real needs of European cities and regions.

- Assessing fundamental rights impact: Given the fact that facial recognition technologies impact a whole range of fundamental rights, it is important to assess them both, to different extents, during the development and the deployment of algorithms.

- Evaluating necessity and proportionality: Prior to deploying facial recognition technology, a city or region must develop a clear understanding of the urban security situation and evidence-based knowledge. The information gathered during a safety audit can help frame considerations of necessity and proportionality in order to find the right balance between the benefits and the risks of using facial recognition technology. This includes an evaluation of which public spaces should be outfitted with the technology for what reasons and problems.

- Monitoring facial recognition technology: When a law enforcement agency uses a facial recognition software, it is paramount that agents verify the results. They should evaluate whether a match is accurate and decide on an appropriate response. The accuracy and efficiency of the software itself should be monitored by independent supervisory bodies.

- A proper understanding of the technology: Local authorities often rely on externally developed technology. In that case it can be both hard to understand how the facial recognition software works and to evaluate it. In order to ensure that fundamental rights, such as the right to non-discrimination and data protection, are integrated not only in the deployment but also in the development of the technology, such considerations must be part of the procurement process (FRA, 2019).

- Adequate police training: Depending on the quality of the software used, it is possible that law enforcement get a large number of hits. The interaction with people who were matched with a face on a watchlist needs to follow the same principles of respect as any other interaction. Again, awareness of the software's potential fallibility and inaccuracy is important in order to understand that a match does not necessarily mean that a person was properly identified or authenticated. Training on how to handle such situations for law enforcement officers can be helpful to ensure calm and dignified interactions with the public.population should also be taken into account.

READING SUGGESTIONS

- In 2019, the French Commission Nationale de l'Informatique et des Libertés (CNIL) published a report on the technical, judicial and ethical elements of facial recognition. It outlines technical, judicial and ethical elements that it deems important to be taken into account.

- In 2019, the European Union Agency for Fundamental Rights (FRA) published a report on fundamental rights considerations of facial recognition technology in the context of law enforcement.

- The EU Commission published a White Paper on "Artificial Intelligence - A European approach to excellence and trust" in 2020.

CCi
CUTTING CRIME
IMPACT

European
Forum *for*
Urban
Security