European Data Protection Supervisor
The EU's independent data protection authority

Facial recognition: A solution in search of a problem?

Monday, 28 October, 2019
Wojciech Wiewiórowski

“Be water”. This is the evocative and enigmatic phrase of the current mask-wearing protestors in Hong-Kong. It seems to represent the fight of citizens for the right to be shapeless and anonymous among the crowd, including when exercising the right to protest, versus surveillance by the state authorities.

It is undeniable that facial recognition, the biometric application used to identify or verify a person’s identity, has become increasingly present in many aspects of daily life. It is used for ‘tagging’ people on social media platforms and to unlock smart phones. In China it is used for airport check-in, for monitoring the attentiveness of pupils at school and even for dispensing paper in public latrines.

In the general absence of specific regulation so far, private companies and public bodies in both democracies and authoritarian states have been adopting this technology for a variety of uses. There is no consensus in society about the ethics of facial recognition, and doubts are growing as to its compliance with the law as well as its ethical sustainability over the long term.

The purposes that triggered the introduction of facial recognition may seem uncontroversial at a first sight: it seems unobjectionable to use it to verify a person’s identity against a presented facial image, such as at national borders including in the EU. It is another level of intrusion to use it to determine the identity of an unknown person by comparing her image against an extensive database of images of known individuals.

In your face

There appear to be two big drivers behind this trend.

Firstly, politicians react to a popular sense of insecurity or fear that associates the movements of foreigners across borders with crime and terrorism. Facial recognition presents itself as a force for efficient security, public order and border control. Facial recognition is a key component of the general surveillance apparatus deployed to control the Uighur population in Xinjiang, justified by the government on grounds of combating terrorism.

The second justification is the lure of avoiding physical and mental efforts - 'convenience': some people would prefer to be able to access to an area or a service without having to produce a document.

France aims to be the first European country to use such technology for granting a digital identity. Meanwhile the Swedish data protection authority recently imposed a fine on a school for testing facial recognition technology to track its students' attendance.
Although there was no great debate on facial recognition during the passage of negotiations on the GDPR and the law enforcement data protection directive, the legislation was designed so that it could adapt over time as technologies evolved.

Face/Off

The privacy and data protection issues with facial recognition, like all forms of data mining and surveillance, are quite straightforward.

First, EU data protection rules clearly cover the processing of biometric data, which includes facial images: 'relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person' (GDPR Art. 2(14)). The GDPR generally forbids the processing of biometric data for uniquely identifying purposes unless one can rely on one of the ten exemptions listed in Art. 9(2).

Second, any interference in fundamental rights under the Article 52 of the Charter must be demonstrably necessary. The bar for this test becomes higher the deeper the interference. Is there any evidence yet that we need the technology at all? Are there really no other less intrusive means to achieve the same goal? Obviously, 'efficiency' and 'convenience' could not stand as sufficient.

Third, could there be a valid legal basis for the application of such technology given that it relies on the large-scale processing of sensitive data? Consent would need to be explicit as well as freely-given, informed and specific. Yet unquestionably a person cannot opt out, still less opt in, when they need access to public spaces that are covered by facial recognition surveillance. Under Article 9(2)(g) the national and EU legislators have the discretion to decide the cases where the use of this technology guarantees a proportionate and necessary interference with human rights.

Fourth, accountability and transparency. The deployment of this technology so far has been marked by obscurity. We basically don't know how data is used by those who collect it, who has access and to whom it is sent, how long do they keep it, how a profile is formed and who is responsible at the end for the automated decision-making. Furthermore, it is almost impossible to trace the origin of the input data; facial recognition systems are fed by numerous images collected by the internet and social media without our permission. Consequently, anyone could become the victim of an algorithm's cold testimony and be categorised (and more than likely discriminated) accordingly.

Finally, the compliance of the technology with principles like data minimisation and the data protection by design obligation is highly doubtful. Facial recognition technology has never been fully accurate, and this has serious consequences for individuals being falsely identified whether as criminals or otherwise. The goal of 'accuracy' implies a logic that irresistibly leads towards an endless collection of (sensitive) data to perfect an ultimately unperfectible algorithm. In fact, there will never be enough data to eliminate bias and the risk of false positives or false negatives.

Saving face

It would be a mistake, however, to focus only on privacy issues. This is fundamentally an ethical question for a democratic society.

A person's face is a precious and fragile element her identity and sense of uniqueness. It will change in appearance over time and she might choose to obscure or to cosmetically change it - that is her basic freedom. Turning the human face into another object for measurement and categorisation by automated processes controlled by powerful companies and

governments touches the right to human dignity - even without the threat of it being used as a tool for oppression by an authoritarian state.

Moreover, it tends to be tested on the poorest and most vulnerable in society, ethnic minorities, migrants and children.

Where combined with other publicly available information and the techniques of Big Data, it could obviously chill individual freedom of expression and association. In Hong Kong the face has become a focal point. The wearing of masks has been a reaction to the use of facial recognition and in turn has been prohibited under a new law.

Does my face look bothered?

It seems that facial recognition is being promoted as a solution for a problem that does not exist. That is why a number of jurisdictions around the world have moved to impose a moratorium on the use of the technology.

We need to assess not only the technology on its own merits, but also the likely direction of travel if it continues to be deployed more and more widely. The next stage will be pressure to adopt other forms of objectification of the human being, gait, emotions, brainwaves. Now is the moment for the EU, as it discusses the ethics of AI and the need for regulation, to determine whether- if ever - facial recognition technology can be permitted in a democratic society. If the answer is yes, only then do we turn questions of how and safeguards and accountability to be put in place.

Independent DPAs will be proactive in these discussions.

Topics:
Technologies