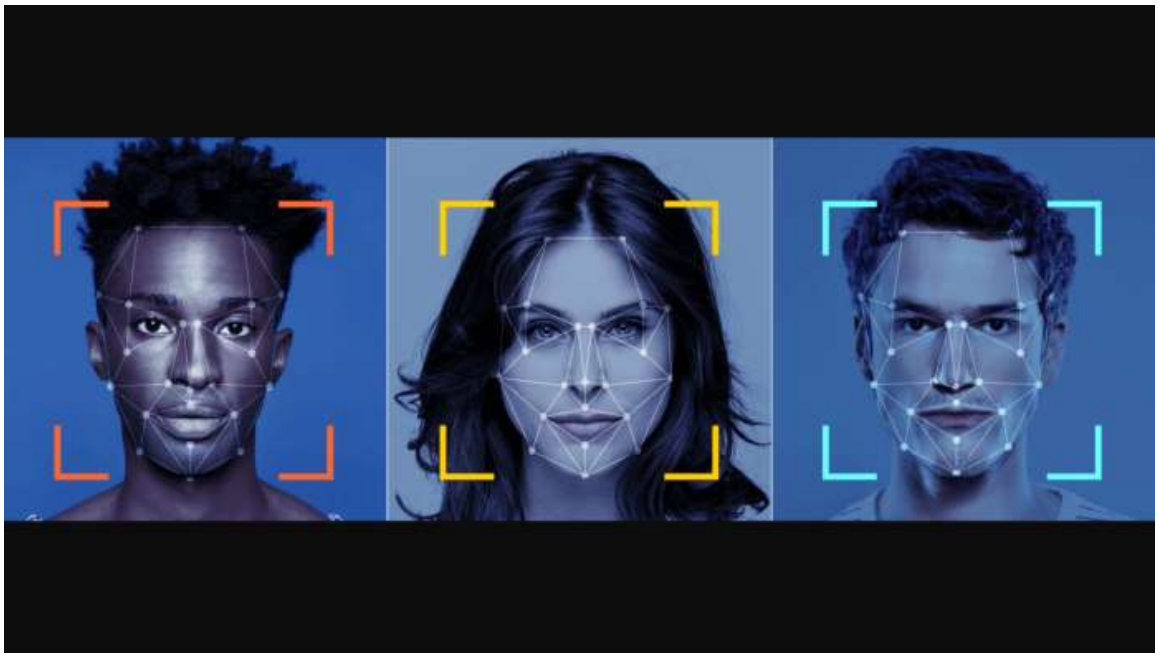
TECH

Security vs Privacy, the problem of facial recognition systems

By **Alessio Caprodossi** January 27, 2022



Cover photo Facial Recognition - @Microsoft

Security and the protection of personal data are the two poles on which the game of video surveillance is played out, a hot topic at the centre of debate in many countries and also among the institutions of the European Union. The latest and most important news on the subject comes from Brussels, with the European Parliament voting at the beginning of October against the use of facial recognition systems in public spaces, with the aim of safeguarding respect for privacy, human dignity and avoiding discriminatory practices. The MEPs' move aims to put forward to the European Commission the establishment of a permanent ban on the use of biometric systems in public spaces and private databases, which are already at the centre of various investigations and blocks established by the authorities to protect citizens' privacy.

Facial recognition, benefits vs risks

When we talk about video surveillance, we are referring to facial recognition techniques, based on the use of cameras that exploit artificial intelligence. "It is a processing of biometric data represented by those unique characteristics of our face that are the so-called nodal points, such as the contour, length and width of the nose, shape of the cheekbones, distance of the eyes, depth of the eye sockets. There are about 80 nodal points of the face and on these we create the template: that is, the faceprint that will be used as a basis for comparison and contrast between the image or video of the individual to be identified and its template/faceprint previously created," explains to *4i-Mag* Alessandro Del Ninno, Lawyer of Tonucci & Partners, Professor of Legal Informatics and Artificial Intelligence, Machine Learning and Law at Luiss Guido Carli in Rome, as well as President of the Scientific Committee of the National Association for the Protection of Personal Data.

Lawyer Alessandro Del Ninno

Facial recognition is a technology that has been used for years to facilitate various aspects of our lives, such as quicker and easier authentication for a range of services, from unlocking a smartphone to opening a hotel room, but its widespread use raises a number of questions because of the risks inherent in certain applications of the same technology.

“Among the advantages we can list are the availability, effectiveness and low cost of the technology. Bearing in mind that with face recognition our body, hence our biometric data, becomes our password. Moreover, there are those who argue that biometrics guarantee higher levels of security, compared to data breaches that can more easily affect ordinary authentication credentials. But the risks can be much greater, to the point that in 2020 the EU proposed a five-year ban on all facial recognition systems.”

It is precisely the risks that force the parties involved to seek a balance between the usefulness and the possible error and abuse associated with the way facial recognition is used and the intent behind its use.“These are systems that are basically used to identify/recognise and classify/categorise individuals, so the criticality known as algorithmic discrimination, an error in the algorithm leading to a discriminatory result in recognition based on age, race, gender is the greatest risk.”

The latter eventuality derives from the different degree of accuracy of facial recognition systems towards different groups: specifically, the effectiveness is very high on white and male individuals, while high error rates in recognition especially of black women and many other minorities. Not forgetting the possibility of error linked to an unrecognised face by virtue of the expression assumed or the camera angle.

Facial recognition – @DedMityay_Adobe Stock

Returning to the focal point on which the issue unfolds, security vs. privacy, it seems complex to find a solution that satisfies the desire to integrate facial recognition in cities by governments, authorities and administrations, while respecting the freedom and rights of citizens. “The proposal for a General Regulation on Artificial Intelligence that the European Union Commission presented on 21 April represents a first, positive regulatory response that looks at guarantees for the security, freedom and rights of citizens by classifying, for example, biometric identification and classification systems among the high-risk intelligence systems for which constraints and requirements will be applied much more stringent than for other AI systems, for their introduction on the market and commissioning,” says Del Ninno.

Why prohibit video surveillance

Many activists and associations opposed to the pervasiveness of technology are urging the European Union to put a stop to attempts to use biometric tools, in particular the use of invasive solutions that, in the name of security, override the privacy of individuals by tracking and analysing faces and bodies while moving in public spaces. “Suspicious incidents have multiplied in recent years and action needs to be taken to prevent them from happening again. The police in Greece using facial recognition to stop migrants, as well as the use of the same technology to monitor the presence of children in a school are cases that, beyond the stop ordered by judges and the national privacy guarantor, must not be repeated,” says Laura Carrer, a member of the Hermes Centre for Transparency and Digital Human Rights, which last year launched the European campaign Reclaim Your Face to ask the European Commission to ban the use of video surveillance tools in public spaces.

A move born from the idea of Brussels’ representatives to renounce the ban on new technologies, considered crucial tools for not losing ground to the rest of the world.”Recent history shows that those who have systems such as facial recognition aim to ride on the coattails of national security and the spectre of terrorist attacks to use the technology, to the detriment of citizens who are neither informed nor aware of the use and consequences of using biometric tools.”

Laura Carrer – Hermes Center

Blocked trials and the importance of GDPR

At least a dozen cities in Italy have planned to install cameras equipped with facial recognition, with the cases of Udine, Turin and Pescara coming to the fore for the impossibility of activating such systems after the block established by the Privacy Guarantor. His decision of 26 February 2020 stopped the Como administration’s project to monitor the area of the city’s railway station, which a few years earlier had hosted hundreds of migrants stranded due to the closure of the border with Switzerland.

For the authority, the acquisition and processing of biometric data had no valid legal basis, yesterday as well as today, with the attempt being finally halted after an investigation by Carrer herself, with fellow journalists and digital rights activists Philip Di Salvo and Riccardo Coluccini.

Given the current rules in Italy, as well as the position taken by the European Parliament, it remains difficult to understand the reasons that drive the supporters of facial recognition to invest money to equip their chosen places with systems that cannot be used. “In the background remains the non-issue of compliance, from the need to comply with the GDPR and the regulations on the processing of biometric data (it should be remembered that the GDPR, as a general rule, prohibits in art. 9.1 the treatment of data of a particular nature, including biometric data), to the need to make the necessary prior assessments of risk, making the so-called Prior Impact Assessment on personal data,” says Del Ninno. “The GDPR is currently the only protection for the space of freedom and security of citizens towards the use of biometric recognition systems and therefore if you do not even comply with the rules data protection, such projects are unlikely to be legal”.