LIVE FACIAL RECOGNITION TECHNOLOGY IS A POTENTIAL THREAT TO PRIVACY: THE KING'S CROSS STATION CASE

EMILIANO TROISI

Key-words: Artificial Intelligence - UK Data Protection Authority - facial recognition technology

Category: Legal Area

The UK Data Protection Authority, the Information Commissioner's Office (ICO), has recently begun an investigation into the use of Facial Recognition (LFR) technology in King's Cross Station of London.

The investigation has come in response to the report of the Financial Times which on 12 August 2019 revealed that a live face-scanning system was in place all across the 67-acre site of King's Cross (including King's Cross and St Pancras stations as well as restaurant, cafes and all the other public spaces) and constantly operated capturing and analyzing people's faces in order to identify suspicious individuals and prevent or detect crime.

The ICO has already expressed concerns about this kind of technology. In early July, Elizabeth Denham, the Information Commissioner, found that Live Facial Recognition technology (LFR) that use AI to scan crowds and then check wide databases for matches in real-time represents a widespread processing of biometric data of thousands of people, so it needs a full justification under the EU's General Data Protection Regulation.

In a very recent statement, the ICO warned that organisations wishing to automatically capture and use images of individuals going about their business in public spaces need to provide clear evidence to demonstrate that it is strictly necessary and proportionate for the circumstances and that there is a legal basis for that use.

The adoption of intrusive facial recognition systems for mass surveillance is alarmingly growing worldwide, both through public law enforcement agencies and private sectors, and so it does the related concern that it could undermine human dignity and fundamental privacy rights because of its potential attitude to interfere with people's private life and their most sensitive data, especially if it is done without people's knowledge or understanding.

This surveillance technology, indeed, since it involves the use of sensitive personal data must always be balanced against people's legal rights; even if it is used in the interest of public safety, organisations using (or wanting to use) LFR for mass surveillance must comply with the EU privacy laws and must do so in a fair, transparent and accountable way, e.g., by ensuring a minimized and strictly necessary processing of data as well as the implementation of technical measures to adequately protect the data collected or assure their timely erasure when become useless.