Facial Recognition Technologies: An Ethical Point of View

Digital Ethics, Università Bocconi

Cesare Bergossi, Giulia Pezzani

May 2023

Introduction

Facial recognition technologies are mainly known for their application in everyday uses, such as smartphone security functionalities. However, these powerful tools have a vast range of applications, from safety concerns to marketing purposes, and are employed especially by entities like government bodies and private companies all around the world.

More specifically, a facial recognition system is capable of detecting human facial features from static and dynamic pictures and matching them with a series of faces collected in a database. This works through software that converts the frames into numerical expressions, implemented to distinguish faces through some kind of algebraical similarity.

It can be considered an adaptive type of technological development since there are no pre-existing societal preferences, yet it modifies and repurposes an existing technology to adjust to changing necessities and predispositions. Indeed, in the past years, we witnessed a transition from systems like fingerprint or retinal identification to this new technology, which had already been implemented but has incredibly been improving using machine learning and computer vision techniques (even if it still has to reach the precision of the pre-existing systems mentioned earlier).

At first sight, it might seem harmless to collective and individual well-being, however, there are many underlying problems to be discussed, especially from an ethical point of view.

Unveiling Benefits

The technical system lying behind this procedure is becoming way faster and more accurate, and can be applied to a myriad of different scenarios, immensely helping with various issues both in the public and private sectors.

A key use for the community's well-being regards public security and crime prevention, one of the main reasons why governments (but also certain private companies) adopted facial recognition. It can identify and track criminals, suspects, and persons of interest, but can go far beyond, finding missing people and children, vulnerable or disoriented adults. Security also concerns airport and border control, for instance, enhancing the efficiency and precision of identity verification processes, while recognizing suspected terrorists and potential threats.

Another strictly related advantage is delivering a more convenient authentication, by using human facial traits as a biometric identifier. First, facial features get uniquely stored in a database, then, when authentication is required, live facial frames get compared to the ones previously captured. Applications of this can be immediately seen in critical areas like banking, where authentication processes are crucial for authorizing transactions or accessing accounts. Simultaneously, it also allows for fraud detection: firstly, this technology allows for a more reliable procedure than using a pin or password, which can easily be stolen and used by hackers. Secondly, by adopting anti-spoofing measures and liveness detection, it is possible to expose attempts of using fake facial images or biometric replicas to deceive the system. While security is one of the main benefits to society, there is much more to it; new approaches using facial recognition and authentication are discovered and studied every day.

Healthcare is among these upcoming research areas: using this kind of technology, it is possible to diagnose diseases and medical conditions by analyzing specific features of the human face (for example, skin conditions, genetic disorders, and early signs of Alzheimer's or Parkinson's).

Lastly, improvements can also be seen in customer service, providing personalized experiences in retail stores or hotels, increasing overall satisfaction, or also in employees' time and attendance tracking, avoiding tedious procedures like manual sign-in and preventing time theft and buddy punching.

Hence, it can be seen how facial recognition has a wide range of fields of application where it can give a huge contribution, simplifying many mechanical processes and being able to improve life quality and welfare. From this point of view, it might seem that this combination of machine learning and computer vision is truly outstanding from an ethical point of view, with its several positive impacts on society. Where is the flaw?

Ethical Pitfalls

All of this indeed comes with a price. This technology presents numerous issues that should not be overlooked.

A first negative implication is the fact that, although it could be useful to track down criminals, facial recognition can easily violate the privacy and civil liberties of ordinary and innocent people, mostly due to the lack of transparency in how information is stored (keeping in mind that databases have the potential to be breached) and managed. This is such a big matter that for instance both Europe and the United States had to implement restrictions banning the use of the software in public spaces, thus creating guidelines on privacy and ethical abuse.

In addition, another cause of concern is the racial bias that the system holds. Although the algorithm has 90% detecting precision, the result is not global. Various assessments, like the one conducted by the National Institute of Standards and Technology (NIST), confirm that various software shows racial bias towards black women. Thus, as an example, in the case of the implementation of facial recognition as a criminal detector, this could lead to false positives, and therefore to the charge of an innocent person.

In turn, the technology could also present a disproportionate effect on ethnic minorities such as immigrants and refugees. These individuals, who generally come from a lower socio-economic status, already have to face injustices within the community, they might also have to cope with unfairness in case of the deployment of facial recognition systems for immigration control or law enforcement. Thus the technology might aggravate already existing inequalities, and lead to unjust persecution and targeting.

Furthermore, governments (mostly the ones with an authoritarian tendency), could employ the software to track and monitor the dissidents. Indeed facial recognition could be used in public places to identify individuals who could threaten authority, and this practice menaces democracy and people's right to have their own opinion.

If this wasn't enough, one last important fact to mention is that this device is not entirely immune to identity fraud; the measures adopted to prevent these crimes could still fail when facing trailblazing cyber intruders. With the information the technology provides, a thief could take out credit cards and open bank accounts in the victim's name. Considering instead the aforementioned use of facial recognition systems to insert offenders on criminal record, threat actors could as well place individuals on a criminal database. Beyond fraud, bad actors could also stalk a person by, for instance, performing reverse image searches on a picture taken in a public place to gather information about their victim and better persecute them.

Facial recognition law has lagged behind potential use by criminals in recent years, which has prompted calls from rights groups for stricter biometrics regulations, to extend to technologies such as live facial recognition.

Drawing Conclusions

To sum up, facial recognition is a useful technology, whose use has been growing exponentially in the last decade, but which carries not insignificant moral implications. The dilemma now is: which criteria should we use to decide whether it is safe enough to be implemented? Alternatively, is the added value associated with it balancing out the potential ethical risks?

There is no universal solution to this problem: ethics is not a manual with definite answers, but rather depends on the subjective point of view, as discussed above.

Two main perspectives through which this concern might be analyzed are consequentialism and deontologism.

The first one morally justifies facial recognition if its benefits exceed the downsides: however, what is a fair classification of good and bad? Once again, this traces back to one of the milestones of ethics, which is investigated more precisely by meta-ethics.

The second one, on the other hand, classifies the moral implications of actions based on preexisting laws and standards, which do not depend on personal opinions, but rather are already part of common sense. Therefore, as opposed to the previous perspective, consequences have no meaning in the moral evaluation of actions, but only their intrinsic virtue is taken into account. Hence, even if the outcome can be considered highly beneficial, the action per se violates moral laws by harming a group of people, thus it should not be considered ethical.

As previously analyzed, the upsides of facial recognition have vast benefits not only on the single individual, but on society as a whole; as a matter of fact, improving safety and assisting in healthcare are remarkable aspects of this type of technology, especially from a consequentialist point of view, as the outcomes yield substantial added value and as a result it could be considered morally correct.

Nonetheless, certain moral conflicts arise, undermining principles and duties upheld by deontological ethics, such as fairness and equality or human dignity. As seen, prominent concerns include violation of privacy and civil liberties, racial bias, disproportionate effects on ethnic minorities, threats to democracy and freedom of opinion, and the potential for identity fraud and abuse.

Which perspective to choose is completely up to the individual, hence the case remains unsolved.