AN ETHICAL FACIAL RECOGNITION: AN OXYMORON?

20/04/2020

Geneviève Fieux-Castagnet and Gérald Santucci

Contents

1. General presentation

How can a machine, even "intelligent", recognize faces? Certainly, all faces have the same elements: two eyes, a nose, lips, forehead, cheeks, ears, hair etc., but at the same time each face is different from that of others and, moreover, the same face often changes appearance depending on the person's age, the emotions they feel, the expressions they give themselves as well as their orientation.

Facial recognition, one of the main applications of artificial intelligence, is gaining ground every day without us even realizing it. Since 2018, travellers who take the train to London from Gare du Nord, or who embark at Roissy-Charles-de-Gaulle, have been dealing with new security gates which are intended to verify their identities whilst passing the border.

Now our faces unlock our cell phones, give us access to our online bank, allow us to board trains and planes, etc.

It goes without saying that the issue of what is happening is important for the respect of our private life. In the age of "surveillance capitalism", to use the expression of American sociologist and academic Shoshana Zuboff, is privacy condemned? Possibly – though it should be noted that "privacy" should not be what "society" (government, business) gives us, but what we decide to do with it.

But beyond privacy, artificial intelligence, and in particular, facial recognition, questions us about ethics. This cross-cutting theme will appear implicitly throughout this article.

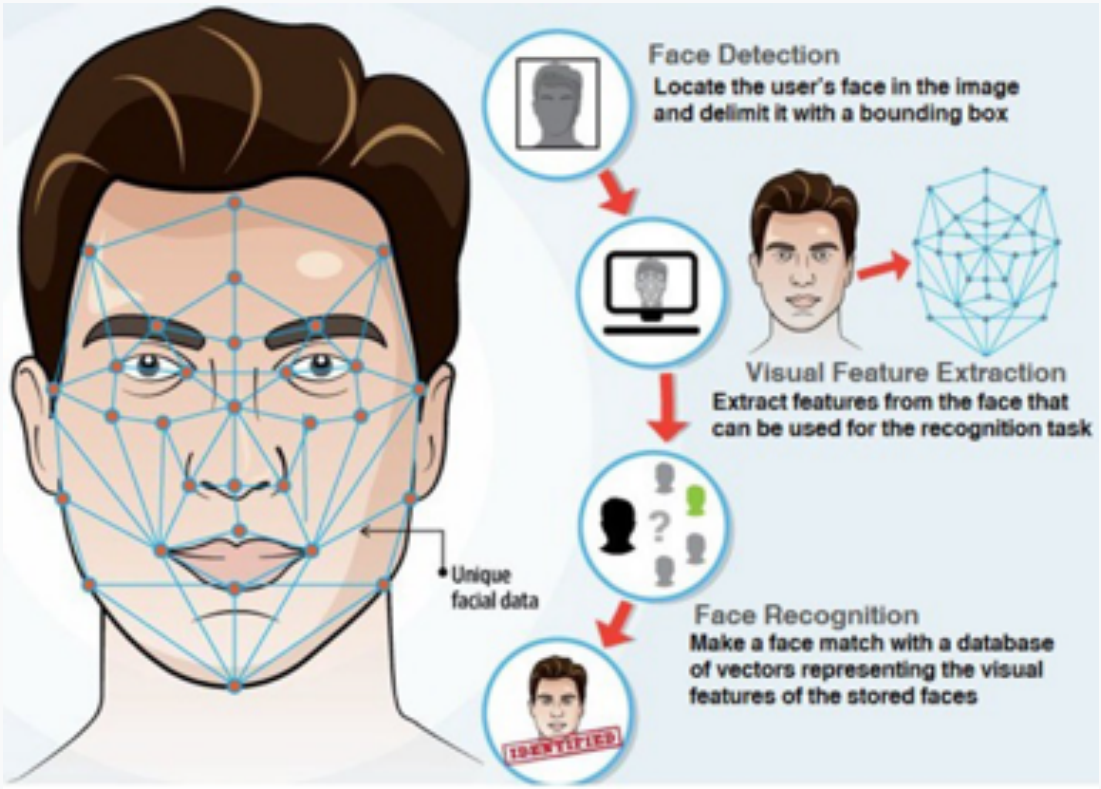
1.1. Technology used

Facial recognition is a computer technology that automatically recognizes a person on the basis of his face. For this, it uses biometric data[1]

The facial recognition is done in four stages:

- Face detection, followed by its alignment, in order to locate the face of an individual on an image and to delimit its contours within a field;
- The extraction of facial features and their computer transformation into a model or template that can be used for the actual recognition task;
- Face recognition by looking for a correspondence between the template and one or more other templates contained in a database.

[1] Biometric data are personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm their unique identification, such as facial images (definition of the General Regulations on the Protection of Personal Data (RGPD) 2016/679 of March 27, 2016).



Source: Youssef FENJIRO, project manager and data science

In the case of facial biometrics, a 2D or 3D sensor "captures" a face, then transforms it into digital data by the operation of an algorithm and compares it to a database.

Thanks to these automated systems, the identification and verification of the identity of individuals can be carried out in just a few seconds from the characteristics of their face: opening of the eyes, edges of the nose, commissures of the lips, ears, chin, etc., including in the middle of a crowd or in dynamic and unstable environments.

Although there are other biometric signatures (fingerprints, iris scan, voice, digitization of veins in the palm of the hand, or behavioural analysis), facial recognition is the most effective references in biometric measurements:

- it is easy to deploy and implement;
- there is no physical interaction required by the end user;
- face detection and matching processes (for verification / identification) are very fast.

1.2. Main functions of facial recognition

Biometrics identify and authenticate a person based on a set of recognizable, verifiable, unique and specific data and can also categorize people.

The identification answers the question: "Who are you?" The person is identified among others by comparing his personal data with the data of other people which are contained in the same database or possibly in linked databases.

It is used in some countries to provide security functions. Facial recognition is used by the police to find criminals, terrorists, lost children etc.

Facial recognition is used by China who has positioned itself at the forefront of facial recognition technology and installed thousands of “smart cameras” across the country. Government and private surveillance companies are partnering to develop surveillance systems. A typical use of facial recognition is the fight against jaywalking in Shenzhen: intelligent surveillance cameras are placed near pedestrian crossings to monitor pedestrian traffic. If a passer-by crosses the signal from the traffic lights without waiting, it is detected by the cameras and the facial data relating to it is compared with that which appears in the files held by the authorities; in the event of a correspondence, the photo of the author of the violation is posted in a general view on a large screen near the pedestrian crossing. In the absence of privacy laws, China has established itself as the world leader in facial recognition. It introduced a “social credit system” which measures the reputation of citizens according to their behaviour and their social presence. The score obtained by an individual defines what he is authorized to do and, below a certain level, certain rights and advantages are taken away from him (for example, the possibility of making a travel reservation).

India, on the other hand, is building the world’s largest facial recognition database. Authorities argue that in a country with 1.3 billion people, this technology is essential to assist the under-resourced police force. In another area, most railway stations plan to use facial recognition software by the end of 2020 to help combat crime. The system is already being tested in the Bangalore technology hub, where half a million faces are scanned each day and then compared to faces stored in police databases. Facial recognition should also be used on board trains by means of video surveillance cameras initially installed inside 1,200 of the 58,000 train compartments. In addition, sensors will be tested to detect certain sounds such as shouts or loud voices emanating from arguments.

Authentication, on the other hand, answers the question, “Are you who you say you are?” Biometrics here is used to certify a person's identity by comparing the data they present with the pre-recorded data of the person they claim to be. Let’s first take the case of the Eurostar. When we previously used this company to go to London, we always had to present our passport and our train ticket. However, everything has changed. The train ticket, instead of being printed on a physical medium, is now an e-ticket downloaded to our mobile phone and, above all, the passport is no longer examined by a security officer at the counter, but checked by a machine whose camera and computer screen scrutinize us: you have to stand in front of the free airlock, position your passport on the reader, then when the passport is detected and the door allows you to enter, the airlock opens, you must position yourself on the ground marking and look at the camera so as to allow the identification of your face. If your face is identified, the airlock exit door opens. In the end, what do we need to take the Eurostar? An e-ticket and a passport, of course, but also and above all a face.

At Aéroports de Paris (ADP), it is the Gemalto company, acquired by Thales in April 2019, which has designed, with the Ministry of the Interior, the computer program known as “Parafe” (Rapid automated exterior border crossing). Thales hopes that its collaboration with ADP will expand to cover all needs from check-in for a flight to the time of boarding, the technology used thus avoiding having to ask for identity items every time.

Categorization by biometrics is used to categorize people according to their characteristics, which include gender, age, ethnicity, in order to profile them. The algorithmic analysis of faces allows detecting certain diseases, such as depression, but also, according to an increasing number of researchers, emotions. Facial expression analysis software like FaceReader is capable of collecting emotion data in order to analyse the expressions “happy”, “sad”, “angry”, “surprised”, “scared”, “disgusted”, and “neutral”. Indeed, capturing emotions by analysing

facial expressions offers additional and objective insights into the impact, appreciation, liking, and disliking of goods, services, mobile apps, websites, commercials, movie trailers, and so on[2]. Because of the vast quantities of data needed to train an artificial intelligence to effectively detect emotions, many researchers remain sceptical about the future of facial recognition in this area, particularly so if the subject is not sitting in front of a camera and looking straight into it. However, new research is being undertaken, for example at Fujitsu where, thanks to what is called a "normalization process", pictures taken from a particular angle can be converted into images that look like a frontal shot. Claiming a detection accuracy rate of 81% (compared to an accuracy rate of 60% for its main competitors), Fujitsu highlights diverse potential applications for its new technology, including road safety by detecting even small changes in drivers' concentration or the capability of a robot to recognize our most subtle changes of humour. such future prospects sound promising indeed, insofar as their ethical implications are effectively addressed, but researchers should bear in mind that face expressions also possess a cultural dimension, i.e. their meaning is different according to where the subject lives – Asia, Europe, Africa or else.

2. Ethical issues

2.1. For use cases involving personal authentication

In this use case, the main ethical risk is a false negative if the person is not recognized, which could lead people to believe that they are not in good standing and thus undermine their dignity. However, we know that false negatives are more frequent among people of colour, which can generate a form of discrimination. Some facial analysis programs are biased by gender or racial bias, which results in a low error rate for light-skinned men, but a high error rate for dark-skinned women[3].

Facial recognition could also be used to access business premises or in high schools. Even if the system was based on the consent of individuals, how can we think that it is really free when there is an unequal balance of power? The use of facial recognition in these cases can very quickly give people the impression of being watched in their behaviour, in their schedules, or in their attendance, which can generate a feeling of surveillance, privacy and individual freedoms.

The collection of biometric data which is one of the attributes of a person's uniqueness can be experienced as an attack on dignity. The more generalized the system, the more there will be a risk of feeling of loss of individuality; the face that expresses a person's emotions and sensitivity will take on the dimension of a simple tool among other tools, thus generating a feeling of "depersonalization" and dehumanization. The raw material of this technology is nothing less than our faces. Can we consider that the face of a user constitutes a "data" like the others?

---

[2] Bartkiene, E.; Steibliene, V.: Adomaitiene, V.; Juodeikiene, G.; Cernauskas, D.; Lele, V.; Klupsaite, D.; Zadeike, D.; Jarutiene, L. & Guiné, R.P.F. (2019), *Factors Affecting Consumer Food Preferences: Food Taste and Depression-Based Evoked Emotional Expressions with the Use of Face Reading Technology*, BioMed Research International, 4, 1-10. https://doi.org/10.1155/2019/2097415

[3] NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software, 19/12/2019, https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software

In addition, misuse or function creep can have serious consequences on the rights and freedoms of people: identity theft, dissemination of images on social networks, blackmail, harassment etc.

As CNIL (*Commission nationale de l'informatique et des libertés*) points out, "facial recognition devices are particularly intrusive and present major risks of invasion of the privacy and individual freedoms of the persons concerned. They are also likely to create a feeling of reinforced surveillance"[4].

All these cases of use of authentication of people generate an addiction and a trivialization of the use of a technology which contains in it the potential for authoritarian drift in an undemocratic regime where the checks and balances would be weak.

2.2. For use cases relating to the identification of persons

A use case can be the identification on the public highway of wanted persons, by confronting in real time all the faces captured on the fly by video protection cameras with a database held by the police. The faces of all the people who pass by or who are there when looking for a specific individual are subjects of facial recognition. The technology, being non-contact, can then be considered invasive. For it to be fully effective in terms of security and tracking offenders, it must still be widely deployed by numerous video cameras equipped with the artificial intelligence system (SIA) and that the databases be the best available. Its effectiveness is therefore proportional to its deployment, which makes this technology an open door to a mass surveillance company.

The mere fact of knowing that one can be the subject of facial recognition in a public place is likely to be experienced as a form of surveillance and interference in the private sphere which can induce behavioural changes and spontaneous restriction in his freedom to come and go, to meet or to associate. This results in a feeling of indirect interference with freedom of expression and, consequently, with privacy and the dignity of the person.[5] Are we ready, as citizens, to completely and permanently lose our anonymity in public spaces? Given the speed of deployment of the multiple uses of facial recognition, what is consent worth? Some people, worried about their privacy, use make-up, clothes and accessories to scramble facial recognition software. "In Russia, an activist artist adept at anti-system performances organized a virtual community around these techniques ... before being arrested."[6]

In addition, facial recognition software in the context of police investigations again presents the risk of "false negatives" (technology fails to match a face with that appearing on a watch list, as a result of which suspects are not detected) and "false positives" (technology leads to identification errors).

Added to this is a significant risk of cybersecurity and malicious data capture which can lead to major risks for individuals, especially when the data is crossed with that of other private databases (for example those of large companies Internet technologies, GAFAM or BATX). Can we trust all those who promise us the security of the ultra-sensitive data that constitutes

---

4 Opinion of CNIL dated October 29, 2019 on a facial recognition experiment in two high schools in the PACA region, https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position

5 "Facial recognition technology: fundamental rights considerations in the context of law enforcement", https://fra.europa.eu/en/publication/2019/facial-recognition

6 https://fr.news.yahoo.com/russie-collectif-d-artistes-dEVELOP-165023862.htm

our face? Who would be able to guarantee the legality of the processing carried out by public or private operators? Consideration should also be given to the case where the controller himself surreptitiously slides from a limited and risk-free use to another more invasive and unauthorized use.

In the case of machine learning, biases could enter and stigmatize part of the population.

2.3. For use cases relating to the categorization of people and their profiling

This use case can help identify categories of people based on their ethnicity. In China, facial recognition has made it possible to identify people of Uighur origin, to follow them, to control them and to lock them up by hundreds of thousands in internment camps. Facial recognition can thus make it possible to exercise repressive action against a minority.

One of the risks of this technology is its combination with other databases which will allow the identification of individuals in very many fields allowing a massive profiling of individuals with a very strong violation of fundamental freedoms and rights[7]. There are already applications that allow you to find the name, activities, contacts of any person from a photo using the billions of data that appear on the internet and on social networks.[8]

The value of AI results depends on the questions put to them: anyone looking for correlations between facies and any type of data will necessarily find them. The exorbitant asymmetry of information implied by this technology increases the possibilities of influence and coercion emanating from the authorities, whether they be political or economic. A "Big Brother" (symbol of totalitarianism) or a "Big Other" (symbol of "instrumentarianism"), capable of recognizing all individuals and instantly obtaining their profile and background, would far surpass the dystopian scenarios imagined. formerly by BF SKINNER (Walden Two, 1948) and George ORWELL (1984, 1949).

Sensing emotions for commercial purposes can also be insidious: smart supermarket shelves raise ethical questions if prices vary depending on the consumer who is in front of them, or even legal questions when personalizing content. without the person's knowledge. Whatever the use case, here again it is advisable to inform well the people who may be subject to automated analyses.

Without prejudging scientific and technological advances which will continue to perfect the uses of facial recognition, it is legitimate to wonder about the real contribution of these systems to improve, as companies claim, "customer satisfaction". Indeed, to what extent is it technically feasible to deduce a degree of customer satisfaction from an emotion? Are our faces not constantly animated by micro-movements which do not necessarily reflect a state of satisfaction or dissatisfaction? In addition, emotions being fleeting, even ephemeral, how could a system capture the moment among so many others during which the emotion expressed is truly a reflection of satisfaction or lasting dissatisfaction? Furthermore, do commercial purposes justify such an intrusion into a person's privacy?

---

7 Under the GDPR, profiling consists of any form of automated processing of personal data consisting in using this personal data to assess certain personal aspects relating to a natural person, in particular to analyze or predict elements concerning work performance, the economic situation, health, personal preferences, interests, reliability, behavior, location or movements of this natural person.

8 Can we fool facial recognition?, Les Echos, March 23, 2020.

3. Towards a framework for the use of facial recognition

The deployment of facial recognition has accelerated in recent years to such an extent that it is legitimate to wonder if it will not end up imposing itself, with its biases on which it will be very difficult to return, despite the discriminations generated, and even though its effectiveness differs according to the conditions of use and the populations (sex, ethnicity, etc.).

3.1. The existing legal framework

Between block rejection of facial recognition and unbridled use, there is a way to find whose responsibility lies with the public authorities. Already in Europe there are "legal benchmarks" which are the European Convention on Human Rights, the Charter of Fundamental Rights of the European Union, the European General Data Protection Regulation and the Police. Justice Directive.

3.1.1. The European Convention on Human Rights and the Charter of Fundamental Rights of the European Union

3.1.1.1. Protected rights

Dignity, freedoms (respect for private life, protection of personal data, freedom of thought, conscience, religion, freedom of expression and information, freedom of assembly and association) constitute by virtue of the European Convention on Human Rights[9] and the Charter of Fundamental Rights of the European Union[10] fundamental rights which must be applied in a non-discriminatory manner.

The protection of personal data and privacy therefore concerns protected rights. Facial recognition using personal data and invading privacy in essence violates these fundamental rights and cannot be developed freely within the European Union. Measures must be taken to ensure that facial recognition respects these fundamental rights.

3.1.1.2. Protection of these rights

The general principle of these texts is that only a law can limit the exercise of the aforementioned rights and freedoms[11].

The limits brought by law to these rights and freedoms must respect the essential content of these rights and freedoms, be necessary, proportional, and meet objectives of general interest recognized by the European Union or the need to protect rights and freedoms of others. The European Convention on Human Rights cites the objectives of general interest which can be, in a democratic society, national security, public safety, the economic well-being of the country, the defence of order and the prevention of crimes protection of health or morals. In light of these texts, facial recognition should not be able to develop outside of a legal framework. In

---

9 European Convention on Human Rights and Fundamental Freedoms adopted on November 4, 1950 and entered into force on September 3, 1953.

10 Charter of Fundamental Rights of the European Union of December 7, 2000.

11 We will not enter into the debate as to whether some of the fundamental rights cannot be subject to limitations as suggested by article 15 paragraph 2 of the European Convention on Human Rights according to which legal limitations are possible for certain rights but not for others because Article 52 of the Charter of Fundamental Rights of the European Union does not make any distinction between rights and provides in general for the possibility of limiting them by law.

France, in particular, there is a European framework with the GDPR and a stricter French framework, authorized by the GDPR[12] with the Data Protection Act.

3.1.2. The general European regulation on the protection of personal data (GDPR)

3.1.2.1. Identification of people

The protection of Article 9 of the aforementioned GDPR clearly provides for the principle of prohibiting the processing of biometric data allowing a person to be identified in a unique way. The principle is therefore the prohibition of facial recognition but only with regard to the identification of people. The ban does not cover the authentication of persons or their classification.

There are exceptions to this prohibition: we will only mention the main ones: first of all, the explicit consent of the persons concerned, which raises the question of truly free consent and the offer of genuine alternatives to facial recognition, and also when a law provides for the possibility of using this technology in public health matters or when there are essential reasons of public interest.

Legal protection is therefore important when it comes to identifying individuals by facial recognition since if the persons concerned do not give their consent, only a law will allow to resort to it. This law must nevertheless respect the principles of the European Convention on Human Rights mentioned above[13].

But what about people authentication and facial recognition profiling?

3.1.2.2. People authentication

In both cases, an impact analysis is mandatory. This impact analysis is indeed required when the processing is likely to create a high risk for the rights of people[14]. It allows an analysis of the impact of the planned processing operations on the protection of personal data. The supervisory authorities draw up lists of the types of processing operations for which an impact assessment is compulsory. In some, the supervisory authority is asked for prior opinion and freedoms of natural persons.[15] The powers of the supervisory authorities are broad: they can request additional information but also carry out investigations and require corrective measures, which can go as far as prohibiting processing and fining in the event of violation of GDPR.

3.1.2.3. Profiling

Profiling using facial recognition to track, for example, the movement of a person and predict its actions is prohibited if it is used to make an automated decision[16]. It is allowed if at the end of the chain there is a human who makes the decision[17].

---

12 Article 9 of the GDPR. Member States may maintain or introduce additional conditions, including limitations, with regard to the processing of genetic data, biometric data or health data.

13 Legal limits must respect the essential content of fundamental rights and freedoms, be necessary, proportional, and meet objectives of general interest recognized by the EU or the need to protect the rights and freedoms of others.

14 Article 35 of the GDPR

15 Article 36 of the GDPR

16 Article 22 of the GDPR

17 Article 58 of the GDPR

However, the law may provide for exceptions to this prohibition.[18]

3.1.2.4. Conditions to be respected

The processing must respect the principles of lawfulness, loyalty and transparency, limitation of the purposes, minimization of data, accuracy, limitation of storage, integrity and confidentiality and these same conditions must be checked with the sub-contractors.[19]

3.1.2.5. Information and access rights

The GDPR provides for a whole series of rights to information and access to data and the non-portability thereof. The use of this technology must be the subject of easily accessible, broad, comprehensible and concise information which must make it possible to know the identity of the controller, the purpose of the processing, its legal basis, the recipients of the data, their shelf life etc. The controller must also provide a right of access, opposition, limitation, rectification, erasure of biometric data by those who are the subject.[20] (these rights may be limited by law, in particular for reasons of public security).

3.1.3. The "Police-Justice" Directive

The GDPR and the Police-Justice directive[21] both make up the "European package for the protection of personal data". They present separate fields of application which are intended to be complementary.

The Police-Justice Directive establishes rules relating to the protection of individuals with regard to the processing of personal data by the competent authorities for the purposes of prevention and detection of criminal offenses, investigations and prosecutions in the matter or the enforcement of criminal sanctions, including protection against threats to public security and the prevention of such threats.

The identification of people from biometric data is authorized in case of absolute necessity. It will take a law to provide for it.

It also provides that the controller must make a clear distinction between the personal data of different categories of data subjects (culprits, those for whom there are serious grounds to believe that they have committed or are about to commit). a criminal offense, victims, witnesses).

3.2. Specific legal treatment of facial recognition

The specificities of facial recognition and its speed of deployment in companies, institutions and civil society make necessary more detailed interpretations of the conditions which are fundamental so that an ethical facial recognition can be developed which benefits everyone without creating new inequalities, without encroaching on public freedoms and without posing new risks to individuals and collective security.

---

18 Article 22 of the GDPR
19 Articles 22 and 23 of the GDPR
20 Article 5 of the GDPR
21 Article 12 et seq. Of the GDPR

At the dawn of the third decade of the twenty-first century, the first elements of what could be a specific legal framework for facial recognition are emerging, while taking into account the fact that Europe is confronted to a triple challenge in this area: a challenge of technological and industrial innovation, a challenge of citizen appropriation and a challenge of legal regulation.[22]

3.2.1. The European Commission's regulatory proposals

The European Commission presented its strategy for artificial intelligence by displaying an ethical approach which it intends to make its marker and its asset, a bit like what happened with the general regulation on the protection of data (GDPR). Moreover, the Danish Commissioner Marghrete VESTAGER, in charge of competition and the digital industry, hit the nail on the head:

"Some say the data is in China and the money is in the United States. But in Europe, we have the purpose and many things on which we can build (…) My approach is not to make Europe more like China or the United States, my plan is to make Europe more like itself." The European Commission has gone back on its intention for a moment to impose a temporary ban on the uses of facial recognition.

It published on February 17, 2020 a White Paper devoted to artificial intelligence[23] in which it supports the adoption of a binding text on artificial intelligence, in particular for high-risk artificial intelligence systems (AIS)[24].

Facial recognition for the identification of individuals is considered by the White Paper as a high risk AIS and should, therefore, be framed by the new regulations envisaged by the Commission. This one which should lay down binding rules in matters:

- control of the data used during training and when using the AIS;
- preservation of archives explaining the choice of data and algorithm;
- information due to the user, in particular on the purpose of the AIS, its capacities and its limits;
- security and accuracy of the AIS, in particular on the reproducibility of its results and its ability to correct errors;
- human action and human control, in particular by validation or appeal by humans of the decisions taken by the SIA, depending on the case by the possibility of imposing constraints or by a stop button.

The Commission's draft White Paper on Artificial Intelligence contains two risk-based approaches: one for the determination of debtors, the other for the establishment of a regulatory framework.

---

22 BAICHÈRE (Didier), Member of Parliament for Yvelines, and SÉJOURNÉ (Stéphane), Member of the European Parliament, "For an ethical facial recognition", Le Monde, 24/10/2019, https://www.lemonde.fr/idees/article/2019 /10/24/pour-une-reconnaissance-faciale-ethique_6016693_3232.htm

23 Brussels, 02/19/2020, COM (2020) 65 final, White Paper "Artificial intelligence – A European approach based on excellence and trust".

24 According to the European Commission, an AI application should generally be considered to be high risk based on what is at stake, examining whether significant risks are associated with both the industry and the intended use.

One of the main difficulties generated by artificial intelligence is the traceability of an error causing damage, due in particular to the diversity of economic actors who are involved in the life cycle of an artificial intelligence. In order to determine who will be held responsible for artificial intelligence, the Commission proposes an approach based on the designation of the person most likely to answer it. Thus, the developer would be most able to respond to the risks generated during the development phase. However, the responsibility of the user will prevail during the use phase.

It also refers to the use of a prior assessment of conformity with test, inspection or certification procedures and ex post control by the competent authorities.

3.2.2. CNIL positions

CNIL, an independent French authority responsible for fundamental rights in the field of biometric data, issues opinions on draft laws or decrees wishing to authorize the use of facial recognition for both identification and authentication of people.[25]

It establishes and publishes standard regulations with a view of ensuring the security of personal data processing systems and governing the processing of biometric data. In particular, it has drawn up binding standard regulations on biometrics in the workplace[26].

Processing in accordance with the standard regulations mentioned in c of 2 ° of I of article 8 of the Data Protection Act implemented by employers or administrations relate to biometric data strictly necessary for controlling access to places of work as well as the devices and applications used in the context of missions entrusted to employees, agents, trainees or service providers[27].

3.2.2.1. The requirements of CNIL in terms of testing facial recognition

CNIL does not oppose in principle the use of facial recognition, however it highlights several requirements to frame the experiment, in particular with regard to respecting the privacy of citizens.

For CNIL, it is important that the experiments do not have the purpose or the effect of accustoming people to intrusive surveillance techniques. While waiting for a legal framework, it wants to avoid that an experiment that does not require legal authorization to date allows a habituation by citizens to unnecessary or non-legitimate uses, or even the development of unwanted uses in any illegality.

An important methodological aspect for CNIL is that the treatments with biometric data are subject to an impact analysis[28] prerequisite which must provide a systematic description of the

---

[25] Article 32 of Law No. 78-17 of January 6, 1978 relating to data processing, files and freedoms: "Are authorized by decree in the Council of State, taken after reasoned and published opinion of the National Commission for Data Processing and freedoms, the processing of personal data implemented on behalf of the State, acting in the exercise of its prerogatives of public power, which relate to genetic data or to biometric data necessary for authentication or to control the identity of persons."

[26] Processing in accordance with the standard regulations mentioned in c of 2 ° of I of article 8 of the Data Protection Act implemented by employers or administrations relate to biometric data strictly necessary for controlling access to places of work as well as the devices and applications used in the context of missions entrusted to employees, agents, trainees or providers.

[27] Article 8b of Law No. 78-17 of January 6, 1978 relating to data processing, files and freedoms.

[28] Deliberation n ° 2018-327 of October 11, 2018 adopting the list of types of processing operations for which a data protection impact assessment is required.

processing operations envisaged and their purposes, carry out an assessment of the necessity and proportionality of the processing operations with regard to the purposes as well as an assessment of the risks to the rights and freedoms of persons concerned, and indicate the measures envisaged to deal with these risks[29]. The impact analysis must be sent to CNIL in the event of high residual risks despite the measures envisaged by the data controller concerned, which will generally be the case with facial recognition.

CNIL is favourable to the fact that the experimentation of facial recognition is the subject of a legal framework and that this framework is the occasion to draw "red lines" of prohibition beyond which no use, even experimental, would only be admitted. These red lines are in line with the requirements posed by the aforementioned legal texts, namely: legitimacy of the aims pursued, minimization of the use of this technology which must be strictly necessary with the demonstration of the inadequacy of other less intrusive means of security, proportionality of uses.

3.2.2.2. Identification of the strictly necessary nature of facial recognition compared to other possible technologies

In the case of use of facial recognition to authenticate in the workplace, CNIL requires that the badge system be not sufficient, that it does not only meet a need for comfort, and that the premises are particularly sensitive.[30]

Less intrusive solutions should be preferred. For instance, it was considered illegal to use the facial recognition system in two high schools of in the South Region. Instead, less intrusive systems such as badges were preferred and implemented.

SNCF therefore chose not to use a facial recognition system in its stations to identify owners of abandoned baggage or perpetrators of flagrant crimes, but rather to use a recognition system through clothing, which is much less intrusive since no biometric data is used to identify the person. This system will soon be taken up by the town hall of Nice and that of Marseilles.

According to CNIL, this approach to finding alternative solutions must be systematized in order to prevent such a highly invasive technology, which generates addiction, from spreading when it is not essential[31].

---

29 Deliberation n ° 2018-326 of October 11, 2018 adopting guidelines on data protection impact assessments (AIPD) provided for by the general data protection regulation (GDPR).

30 Deliberation n ° 2019-001 of January 10, 2019 relating to the standard regulation relating to the implementation of devices having for purpose the access control by biometric authentication to premises, devices and computer applications in the workplace.

31 At the time of the outbreak, several Asian countries implemented mobile applications to track the spread of Covid-19 or limit the movement of infected people. In China, Ant Financial, a subsidiary of Alibaba, launched the Alipay Health Code application on February 11, 2020: based on the user's travel history and a questionnaire on their state of health, an algorithm evaluates the risk that he has been in contact with other carriers of the virus. The result is displayed in the form of a QR Code which can have three colors: green, the risk is low, and the user can move around; yellow, the person must remain confined for seven days; red, she must observe fourteen quarantine days. In the most affected regions, the code is checked at all times, on the street or in transport. In South Korea, the Interior Ministry launched a quarantine monitoring app in early March. It allows the authorities to be kept informed of developments in their state of health, but also to ensure that they respect confinement. In Singapore, the TraceTogether app uses the Bluetooth antennas of smartphones instead of GPS to record any encounter between two people within a radius of about 2 meters. Outside of Asia, Israel and Iran have announced the adoption of similar technologies. As for Poland,

It is interesting to note that rather than using facial recognition to identify the movements of people with the SARS-Cov-2 (COVID-19) disease, some countries have used other less invasive technologies, in particular "contact tracing" solutions, that is, tracking potentially contaminated people.

In France, CNIL agrees that we measure population movements using data from telecom operators (this is how it was possible to assess that 1.2 million Ile-de-France residents had left their region at the start of confinement), but she does not agree to establish individual monitoring, unless this is based on a voluntary approach by the person concerned.

3.2.2.3. Seeking real consent

CNIL recalled on several occasions that consent could only be free "if the processing of data was strictly necessary for the provision of the service requested by the person, or if an alternative was actually offered by the controller to the data subject." The latter implies that the citizen, the user or the consumer should be able to choose between using a system with facial recognition or using another system.

This is the case in the Parafe intelligent airlock system, with users being able to choose to adopt it or go through conventional border control. This freedom should be able to be exercised over time and not just as long as people get used to using facial recognition. Going back should also be made possible.

However, how can we be sure that the individual's consent is "real"? Can the person who gives his consent be the victim of a lack of information or of a "soft manipulation" (nudge)?

The alternative solutions proposed, such as for example the smart airlocks in airports, are they not unbalanced since the solution based on facial recognition is much more effective than any other (speed, ease of use, etc.)?

Over the years, the waiting time at border crossings has tended to increase due to the tightening of controls by the authorities and staff which have not changed. How can we believe that the "progress" generated by the Parafe facial recognition system, in terms of speed (10-15 seconds versus 30-45 seconds for the old fingerprint system) and security could be rejected by the vast majority of users? We have to face the facts: facial recognition solutions, applied to smart airlocks at airports or to other security control procedures, will impose themselves easily and irreversibly as soon as they undoubtedly translate into gains. performance and cost reductions.

3.3. Technical measures for securing data or algorithms

Facial recognition technology, as we have seen, has its ramifications throughout the economy and civil society. Police around the world are implementing programs using cameras to scan crowds at matches in football stadiums, festivals, and street protests, with the aim of identifying persons suspected of an offense. For their part, the digital giants are shamelessly entering the game: Facebook relies on facial recognition to label our photos automatically; Snapchat uses it

---

it already requires, via an application, people in quarantine to send geolocated selfies. These technologies have proven to be quite effective, but they pose real problems in terms of public freedoms in Western democracies. An analysis by the New York Times of the Alipay Health Code source code showed that the program was sending data to Chinese police servers. In Korea, where the tracking app is coupled with alerts sent to the population by SMS, several people have been publicly identified - and not surprisingly stigmatized.

to overlay fun animations on our face; Apple uses it to unlock our cell phones via FaceID (its facial verification system); Amazon uses an image analysis system, Rekognition, which allows, between other things, real-time facial recognition among tens of millions of faces.

Regulators around the world recognize the importance of respecting privacy and require that "personally identifiable information" (PII) be protected, hence the European General Data Protection Regulation (GDPR, 2016) , the law passed by the United States of Illinois on the protection of biometric information (Biometric Information Privacy Act, or BIPA, 2008), or the American law on portability and liability in health insurance (Health Insurance Portability and Accountability Act, or HIPAA, 1996). Under the GDPR, facial images are sensitive personal data which are subject to requirements and restrictions. Companies are therefore encouraged to use technical measures to comply with the principles of the GDPR, including default confidentiality, the right to be forgotten or even the protection of privacy by design.

In addition to the regulatory arsenal, technical measures to limit attacks on privacy, personal data and public freedoms are beginning to be implemented.

The risk of theft or misuse of use will be limited if the biometric data is stored by the person himself. This is the case in the Parafe system since the biometric data is contained in the chip integrated in the biometric passport, which makes it possible to limit the risks of data theft.

In addition, the shorter the data retention period, the less important the risk of theft or misuse of use: in the Parafe system, the images collected are deleted as soon as they are compared with the image scanned and stored in the passport.

It will also be necessary to systematically detect biases in the databases and in the algorithms in the event of machine learning and correct them regularly so as to prevent undue discriminatory processing.

There are ways to limit cyber security risks:

- the use of dedicated computers accessible only in secure premises (badge required, etc.);
- partitioned video networks (by VLAN etc.);
- installing antivirus and other protection on computers;
- dedicated workstations, connected to secure networks;
- the use of dedicated and trained staff;
- strict control of the providers accessing the data;
- data traceability and logging;
- internal archiving and maintenance.

We are only at the beginning of innovation in the fields of security and cybersecurity concerning facial recognition algorithms and artificial intelligence systems in general. In the near future, companies will not only have to scrupulously respect the laws, more or less severe depending on the country and no doubt ever-evolving, but also to develop an arsenal of specific protections combining technical, organizational and management measures.

4. Facial recognition and democratic life

4.1. The launch of national and European debates

A consensus seems to exist, at least in Europe, on the point that the questions relating to the analysis of the faces, in particular by the use of deep learning, should not remain only in the hands of the engineers and the companies. AI confers powers hitherto inaccessible which justify that facial recognition, which carries the risk of mass surveillance, is the subject of an open, inclusive and participative debate.

European Commission supports European debate

The European Commission launched a consultation on February 19, 2020, which notably focused on the specific circumstances enabling the use of facial recognition to be identified to identify people in public places as well as on the common guarantees to be put in place. This consultation will end on May 31, 2020.

CNIL favours a national debate

CNIL wishes to contribute to the debate on facial recognition with several objectives[32]:

- clarify the subject of the debate for all citizens by presenting what facial recognition is technically and what it is used for;
- highlight the technological, ethical, societal risks linked to this technology, by showing in particular that facial recognition can become a particularly ubiquitous and intrusive tool and that data breach or any misuse can generate significant risks (blocking of access to a service, identity theft, etc.); risk assessment is therefore essential to determine which are not acceptable in a democratic society and which can be assumed with appropriate guarantees;
- recall the principles that must frame practices: placing respect for people at the heart of the systems, for example by obtaining their consent and guaranteeing them control of their data and access to information; compliance with these principles, which comply with the GDPR, has already led CNIL to admit certain uses while framing their practical methods (border controls at airports, control of access to the Nice carnival) and to refuse the use of others (access control of pupils in educational establishments)[33].

The launch of a broad public debate on what may be exceptional circumstances justifying the use of biometrics will be very useful, but on condition that this debate is not limited to identification by facial recognition but also intended to reflect on the issues related to authentication and categorization by facial recognition. It should allow all stakeholders in civil society to make their voices heard.

---

[32] CNIL, "Facial recognition: for a debate that meets the challenges", 11/15/2019, https://www.cnil.fr/fr/reconnaissance-faciale-pour-un-debat-la-hauteur-des- stakes

[33] CNIL, "Experimenting with facial recognition in two high schools: CNIL specifies its position", 10/29/2019, https://www.cnil.fr/fr/experimentation-de-la-reconnaissance-faciale-dans-deux-lycees-la-cnil-precise-sa-position

4.2. Democratic guarantees of power

As a result of these democratic debates, it should be possible to list the safe use cases, the use cases subject to prior authorization and the use cases prohibited except in exceptional circumstances.

Use cases subject to prior authorization must be examined by independent ethics committees within the Member States, made up of stakeholders and chaired for example by senior magistrates from the seat, these committees working as a network between them. They can rely on their analysis of the seven principles decreed by the European Commission in 2018:

- human factor and human control: AI systems should be the vectors of equitable societies by putting themselves at the service of humans and fundamental rights, without restricting or deviating human autonomy;
- robustness and security: a trustworthy AI requires algorithms that are sufficiently safe, reliable and robust to manage errors or inconsistencies in all phases of the life cycle of AI systems;
- respect for private life and data governance: citizens must have total control over their personal data and data concerning them must not be used against them for harmful or discriminatory purposes;
- transparency: the traceability of AI systems must be ensured;
- diversity, non-discrimination and equity: AI systems should consider the full range of human capacities, skills and needs, and their accessibility should be guaranteed;
- societal and environmental well-being: AI systems should be used to support positive social developments and strengthen sustainability and ecological responsibility;
- Accountability: mechanisms should be put in place to ensure accountability for AI systems and their results, and be made accountable.

The prohibited use cases can only be developed for a limited period of time due to exceptional circumstances of general interest, security or public health which must be voted by parliaments, respecting the essential content of rights and freedoms of the European Convention on Human Rights, be necessary, proportional and subject to the supervision of a judicial authority.

Public auditors should be dispatched to verify that use cases are not diverted and that decisions made within the framework of ethical committees are respected.

5. Conclusion

Facial recognition technology has entered our societies in a fairly subversive way, without real democratic control, without open and prior debates that can circulate, beyond the microcosm of well-informed stakeholders, essential knowledge from the point of view of respect and fundamental human rights. It has imposed itself within a few years at the confluence of technological advances in the field of artificial intelligence and the rapid evolution of needs in the vast space of areas of general interest (safety, mobility and transport, health, etc.).

It would be pointless to pretend to ignore that, as history shows, when a technology becomes available, it ends up being used. However, this does not mean that its use should be left to the whim of anyone, for any purpose, and under any conditions.

In democratic countries, a consensus is emerging in favour of experimentation phases in various use cases, limited in time and in their field of application, in order to inform public debates and guide decision-making.

In the absence of such experiments, we most often find ourselves in situations where the use of facial recognition remains prohibited by law even as local authorities grant more and more exceptions by issuing permits. on an experimental basis.

This article indicated that our societies were faced with a triple challenge: a challenge of technological and industrial innovation, a challenge of citizen appropriation and a challenge of legal regulation. These three challenges must be considered at the same time without one ignoring the other two or minimizing their importance. Compared to the important challenge of privacy, the technological strategies of the countries of Asia at the time of the outbreak of the COVID-19 epidemic were denounced in Europe, less in the United States, because of their incompatibility with our “values” and our laws.

However, the current pandemic as well as other global challenges – climate change, desertification (one third of the total land area), migratory movements, demographic changes, shortages of resources (water, sand, foodstuffs, etc.) – converge to lead us to think that we are witnessing a change of civilization. We are witnessing an “acceleration of history” which forces us to revise our concepts, prejudices, strategies, at the risk of endangering humanity. Individual freedoms, and the fundamental rights that support them, are obviously a legacy of history that humanity must preserve. But wouldn't it be time to also realize to what extent the human person, being singular, also constitutes a node of relations with the others and the planet, which makes him the holder of a share of responsibility vis-à-vis not only generations of humans around him but also of the human species, and therefore vis-à-vis future generations?