Strasbourg, 13 November 2019

T-PD(2019)05rev

CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA

CONVENTION 108

FACIAL RECOGNITION: CURRENT SITUATION AND CHALLENGES

by

Sandra Azria and Frédéric Wickert

DG I – Human Rights and Rule of Law

The opinions expressed in this work are the responsibility of the authors and do not necessarily reflect the official policy of the Council of Europe

TECHNICAL ASPECTS

By Frédéric Wickert,
Lecturer/Consultant/Adviser/Trainer in artificial intelligence
Founder of A.I. SENSE

1. INTRODUCTION

From a technical viewpoint, facial recognition is a subcategory of the sphere of artificial intelligence[1] known as “computer vision”.
The aim of computer vision is to create algorithms to extract information from images with a view to identifying objects (with keywords or tags), detecting objects and their position in images, detecting brands, categorising images, describing images, and detecting faces, celebrities, geographical features, colour schemes, text, and inappropriate images. However, it can also be used to analyse faces (detecting people’s gender or emotions or the accessories they are wearing) or to identify faces. The latter use, known as facial recognition, will be the focus of this report.

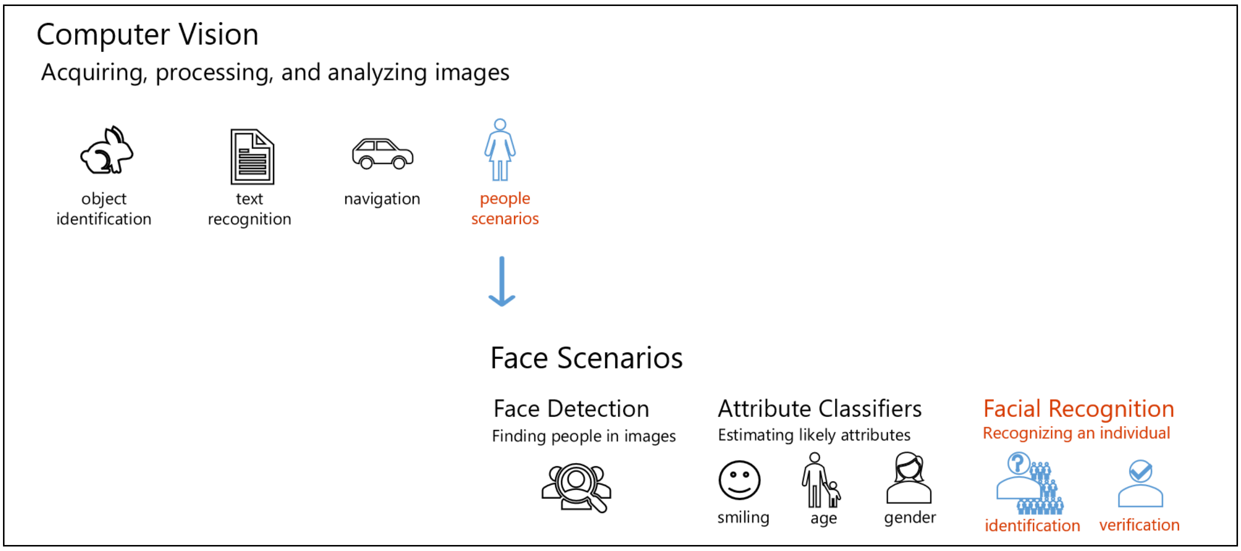


Figure 1: Computer vision

2. GENERAL FUNCTIONING

When dealing with the above scenarios it is very difficult to devise a deterministic algorithm,[2] as it would require developers to propose an almost infinite management of the possibilities arising from the volume and variety of images on which to establish their algorithm. And even if they managed to do this with one image, their algorithm would not be suited to other images. This raises the question of how one should go about coding the action of detecting a face on a photo. What combinations of pixels mean that it can be deduced that there is a face in an image or not?
The solution is to use algorithms based on Deep Learning and Deep Neural Networks.
The idea here is not to enter into the detail of how Deep Learning works, just to highlight certain points.

[1] The term “artificial intelligence” is currently very fashionable and many digital service businesses claim to offer artificial intelligence solutions.
However, when we look in detail at these, it becomes clear that what they are actually offering is “business intelligence” or “data science” services (without predictive algorithms). Moreover, it is difficult today to gain a clear picture of the typography of artificial intelligence providers, their scope of application and activity, their ethical standards and other aspects.

[2] In other words, those that are used for management applications based on conditional instructions such as “if” statements and “while” loops.

Firstly, what makes artificial intelligence algorithms and techniques different from deterministic algorithms is that they are “probabilistic” – they are said to be “stochastic”.[3]

An important thing to retain is that an AI algorithm can never be expected to produce a response that is 100% reliable. To expect anything else would be entirely utopian.

Secondly, to arrive at the most accurate answer possible, the algorithm must learn to find the right answer. For example, it must “learn” to detect a face in a photo. “Learning” here means that the neural network builds the “model”[4] to detect faces. For this purpose, it will be provided with input information consisting of images and the response to a question – for example 10 million photos producing the response: “yes, there is a face” and a number of photos without faces.

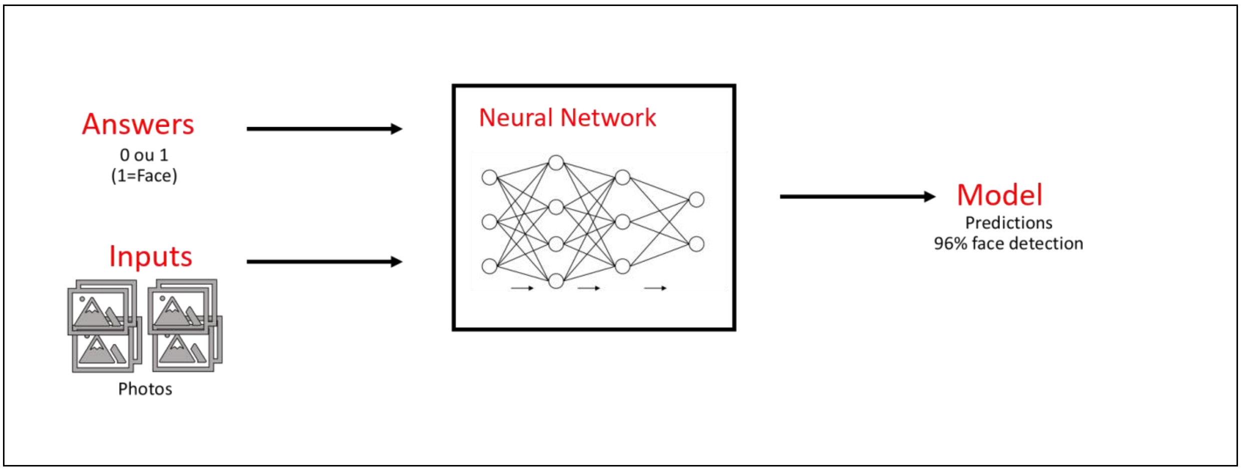


Figure 2: Neural network learning

In this way, the neural network will learn (hence the term Deep Learning) how to detect a face in a photo basing itself on so-called training data. This process of creating a model may take hours, days, weeks or months (depending on the number of images in the training set, the complexity of what is required and the minimum level of reliability desired).
The process is repeated for all the other use scenarios (analysing faces for emotions, age, gender, etc.).
Once the training phase is over and the model has been created, it can be supplied to developers, who can then incorporate the function into an application on the web, a mobile, a camera or another device. The process can be summed up as an iterative cycle.

[3] Which is to say that the result will be expressed as a probability of the accuracy of the answer, the aim being to get as close as possible to 100%. “I am 87% certain that there is a face in this image and 67% certain that it is smiling”.
[4] The model will be the finalised algorithm, which will find the solution with a specified degree of accuracy.

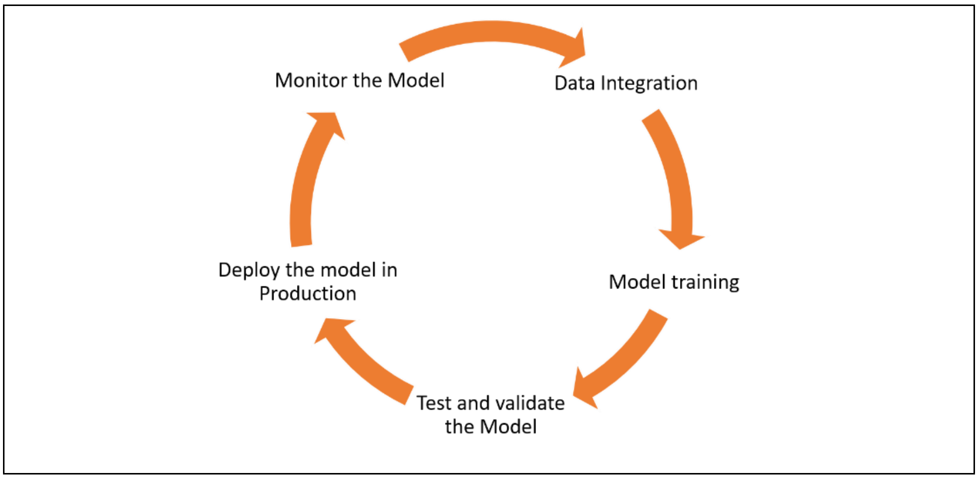


Figure 3: Iterative AI model development cycle

For each version of the model, new photos can be incorporated, and another neural network architecture can be used. This will influence the result, the goal being to improve reliability rates and minimise biases.

3. REQUISITE TECHNICAL PROFILES

Human expertise in the creation of algorithms for face detection, facial analysis or facial recognition can be broken down into three types of profile: AI researchers, data scientists and developers.
AI researchers determine the neural network architecture and the neural behaviour which work best for a specific purpose.[5]
Data scientists incorporate data (photos and responses) and use these architectures to create the programme which will generate the model. Subsequently, they deploy the model.
Developers use the model created to incorporate functions into their application.

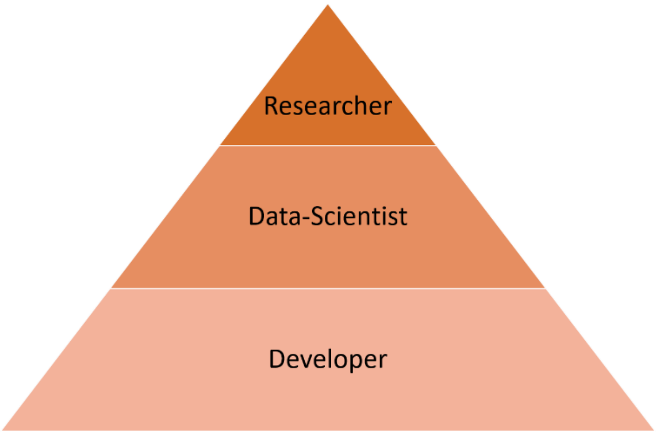


Figure 4: Pyramid showing the relative numbers of professional profiles.

Although the three profiles complement one another, they do not need to be deployed in the same company or the same group.
Most AI researchers work for university laboratories or the major private firms such as the Big Six (Google, Amazon, Facebook, Apple, Microsoft, IBM) (in the United States) or Baidu, Alibaba, Tencent or Xiaomi (BATX) (in China), and their data scientists make their models available to developers throughout the world (either free of charge or for a fee).

Developers have two choices, either to build their own model or to use models that have already been trained.

[5] A "bestiary" of neural networks can be found here: http://www.asimovinstitute.org/neural-network-zoo/

4. BUILDING ONE'S OWN MODEL

To build one's own model, for example to detect a face in a photo (which is a prerequisite for facial recognition), the following are needed:

- a data set: photos of faces and labels;
- powerful computers to train the model;
- computers to deploy the model for it to be used.

4.1 Data sets

Data sets can be found on many platforms. On the Face Recognition Homepage (http://face-rec.org/databases/), you will find a list of data sets designed specifically for facial recognition. They contain photos and labels (the answers) to train deep learning algorithms. The life cycle of such data must be managed, in other words, the data must be collected, stored, audited, kept safe, etc., in compliance with the GDPR.

4.2 Training

To train an artificial intelligence model, powerful machines are used, which are made up of specific technical components (a GPU graphics card and new generation processors such as FPGAs or TPUs[6]).
This type of machine can of course be bought or rented from a public Cloud supplier such as Amazon Web Service, IBM or Microsoft (for FPGAs) or Google (for TPUs).
To simplify the creation of models, libraries are used (which are often open source) such as OpenCV, Tensorflow, CNTK and others.[7]

4.3 Deployment

Models can be deployed on a web application, a mobile application (iOS or Android) or on connected objects such as cameras or drones.

At all events, building one's own model requires considerable expertise, calling for the skills of a data scientist.

5. USING TRAINED MODELS

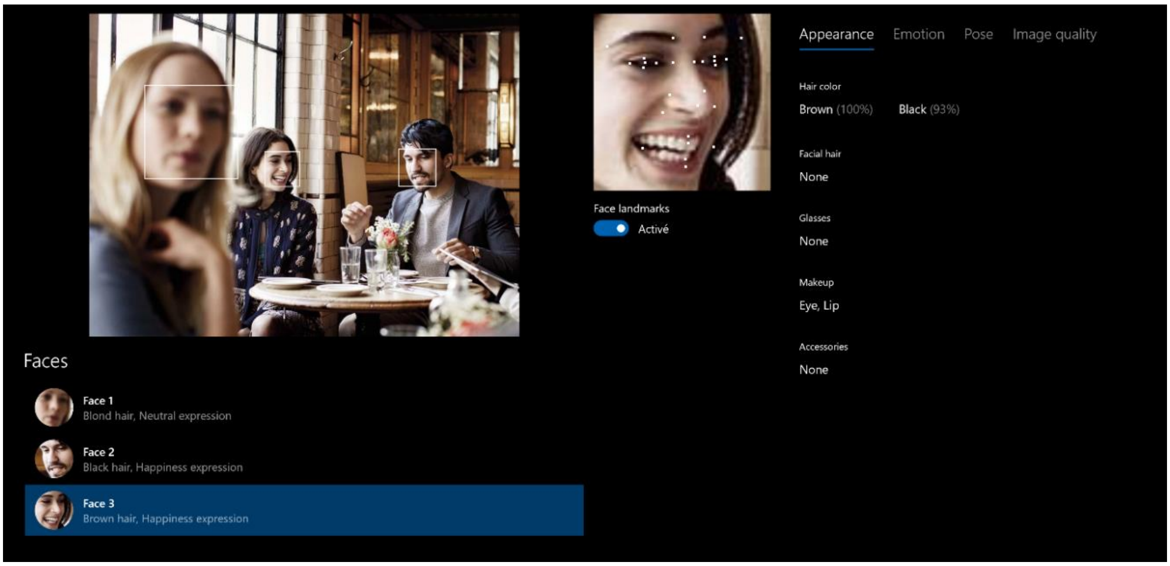
For those who do not have the data or the skills to create their own model, there is a means of using facial recognition (or any other type of model involving faces). Some companies make their trained models available in the form of Web APIs, which can be accessed by all developers. This is the case with some of the Big Six companies[8] such as Amazon Web Service (https://aws.amazon.com/fr/rekognition/) and Microsoft (https://azure.microsoft.com/en-us/services/cognitive-services/face/) or the specialist company, Kairos (https://www.kairos.com).

Here is an example of how one of these APIs can be used in the "Microsoft Kiosk" application.

[6] FPGA: https://en.wikipedia.org/wiki/Programmable_logic_device and TPU https://en.wikipedia.org/wiki/Tensor_processing_unit

[7] Some open source projects using these libraries: https://awesomeopensource.com/projects/face-detection

[8] Google, Apple, Facebook, Amazon, Microsoft, IBM



Faces

Face 1
Blond hair, Neutral expression

Face 2
Black hair, Happiness expression

Face 3
Brown hair, Happiness expression

Face landmarks
Activé

Hair color
Brown (100%) Black (93%)

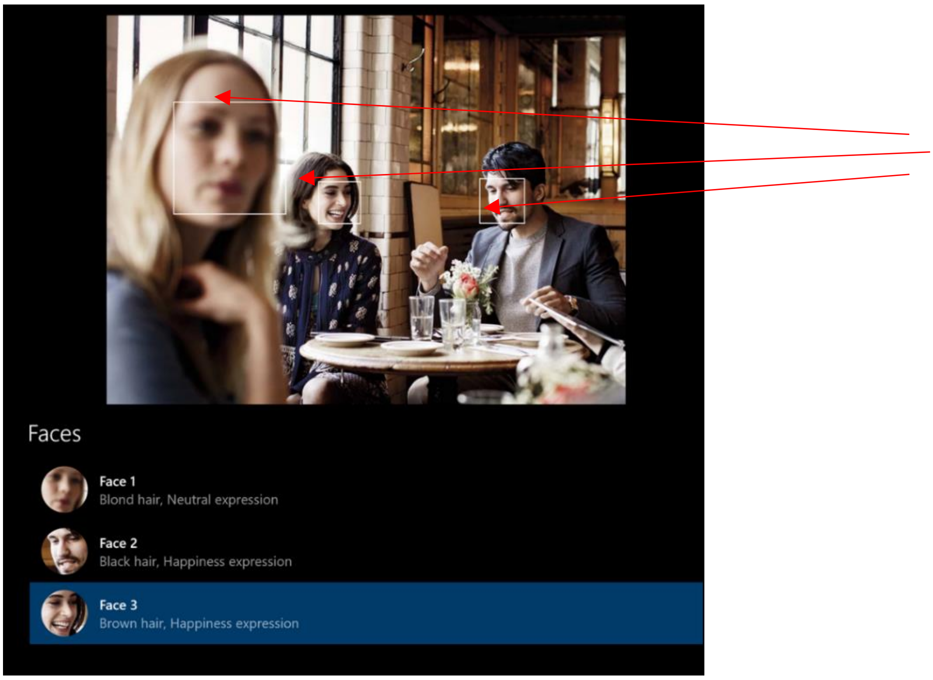
Facial hair
None

Glasses
None

Makeup
Eye, Lip

Accessories
None

Figure 5: Microsoft Kiosk application used to test cognitive APIs



Faces

Face 1
Blond hair, Neutral expression

Face 2
Black hair, Happiness expression

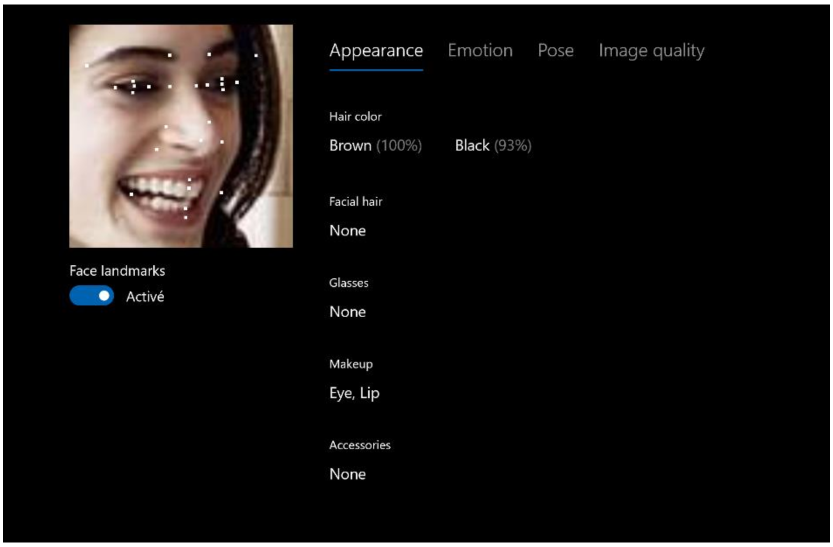
Face 3
Brown hair, Happiness expression

3 faces have been detected in the photo

Figure 6: detection of faces

5.1 Appearance

- 27 dots outline the face through the position of the eyes, nose and mouth.
- Hair colour
- Whether the face is obscured by the person’s hair
- Accessories such as glasses
- Make-up on lips and around eyes, for example.



Face landmarks

Activé

Hair color

Brown (100%) Black (93%)

Facial hair

None

Glasses

None

Makeup

Eye, Lip

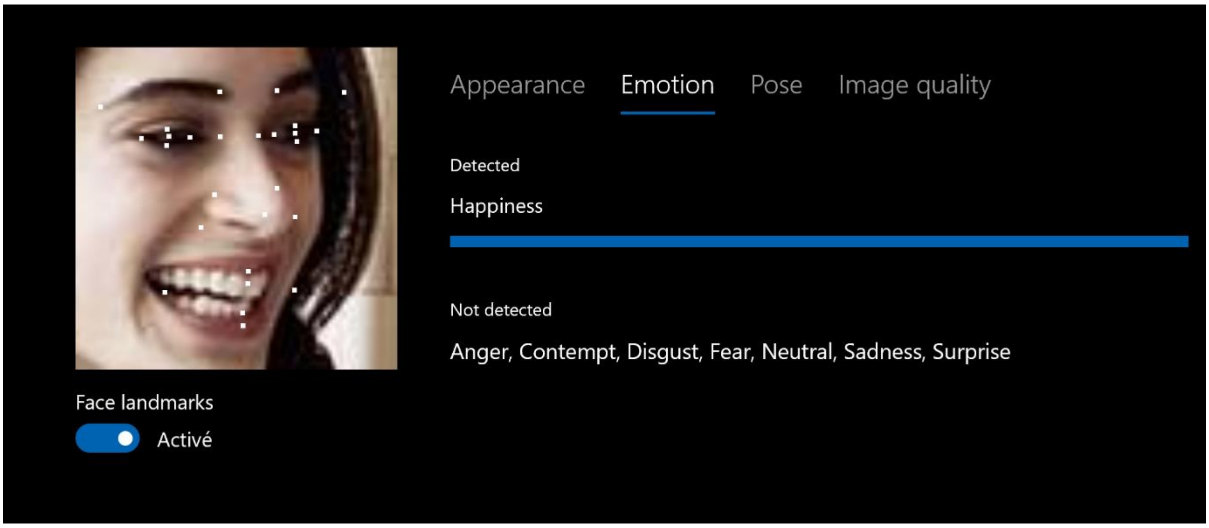
Accessories

None

Figure 7: appearance analysis

5.2 Emotions

8 emotions can be detected: happiness (here at 100%), anger, contempt, disgust, fear, sadness, surprise or neutral.



Detected

Happiness

Not detected

Anger, Contempt, Disgust, Fear, Neutral, Sadness, Surprise

Face landmarks

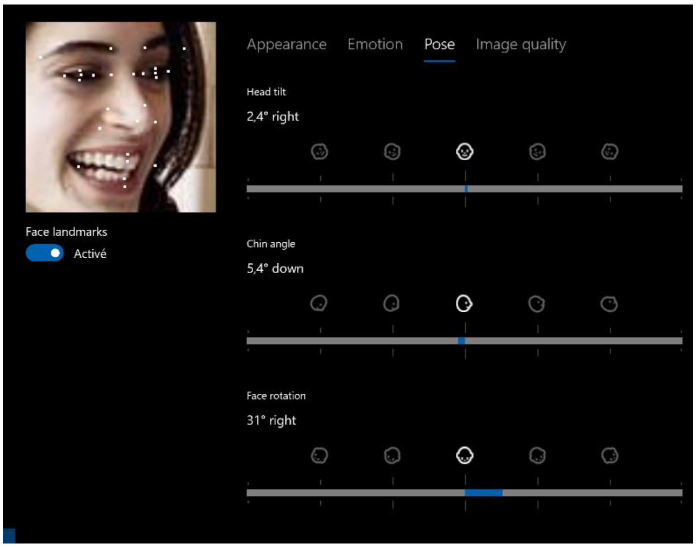
Activé

Figure 8: emotions analysis

5.3 Pose

Position of the head:

- Head tilt
- Chin angle
- Face rotation



Head tilt
2,4° right

Chin angle
5,4° down

Face rotation
31° right

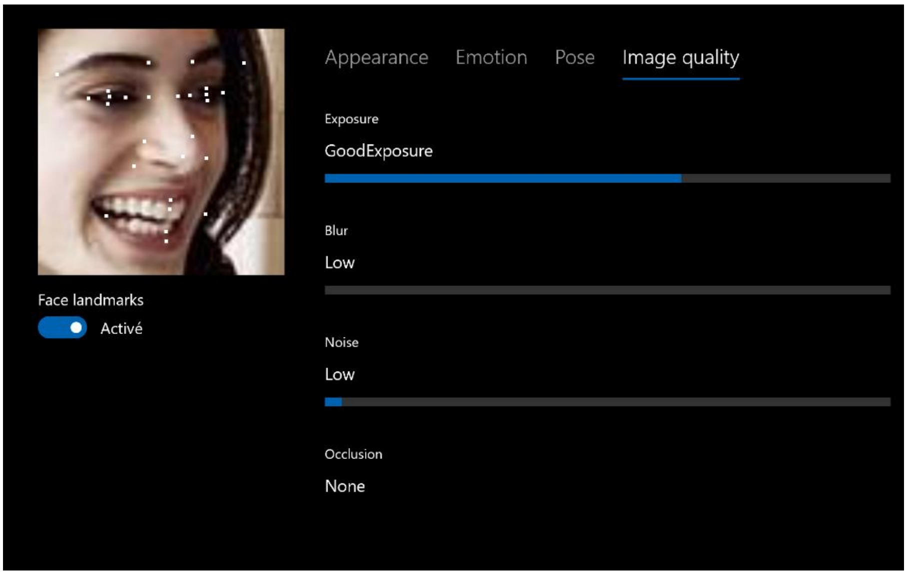
Face landmarks
Activé

Figure 9: analysis of the position of the head

5.4 Quality

Image quality:

- Exposure
- Blur
- Noise
- Occlusion



Exposure
GoodExposure

Blur
Low

Noise
Low

Occlusion
None

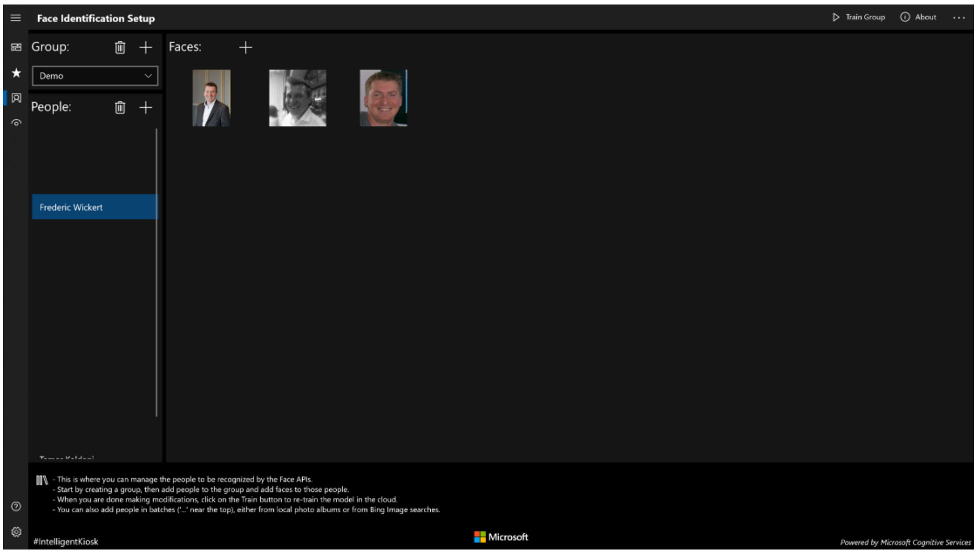
Face landmarks
Activé

Figure 10: analysis of the quality of the input picture

In this case, developers do not have to do any training; they simply have to send in an image to be given all these details. The tool is very simple to use and can be integrated into any application: web applications, mobile applications, cameras, drones, etc.

6. IDENTIFICATION

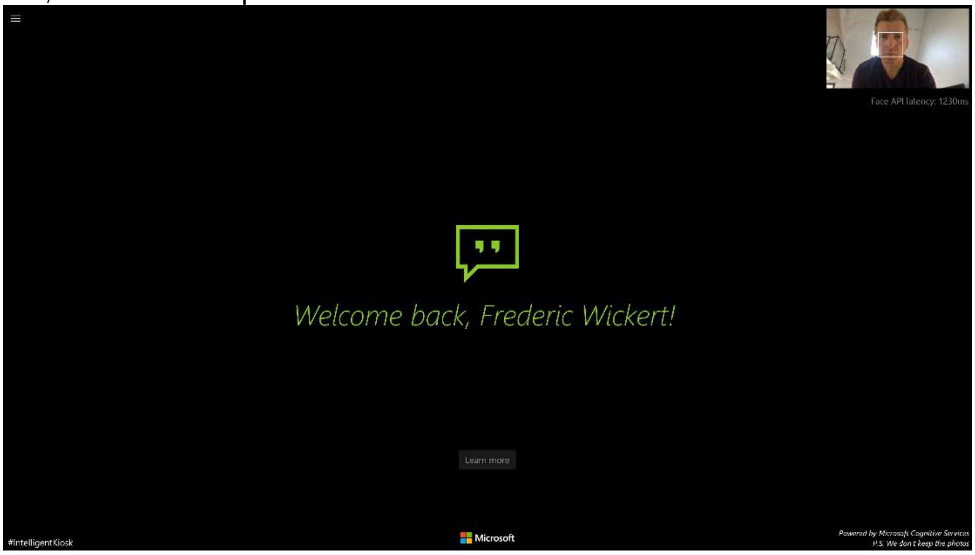
We have seen how algorithms now enable us to collect a large amount of information on faces in a photo or a video. For the purposes of identification, we simply have to compare a face found in a photo with images in a database.
An intermediate stage must then take place, which is to train a model using photos of faces and their name (or identifier). One photo may then be enough to make a match. Of course, several photos will enable a better match to be made (particularly if the photos have been taken from different angles).



- This is where you can manage the people to be recognized by the Face APIs.
- Start by creating a group, then add people to the group and add faces to those people.
- When you are done making modifications, click on the Train button to re-train the model in the cloud.
- You can also add people in batches ('...' near the top), either from local photo albums or from Bing Image searches.

Figure 11: 3 faces have been used in this case to recognise this person

Once the faces and the responses have been recorded, training takes a few seconds and following this, identification is possible.


Learn more
#IntelligentKiosk
Microsoft
Powered by Microsoft Cognitive Services
P.S. We don't keep the photos

Face API latency: 1230ms

Welcome back, Frederic Wickert!

Figure 12: identification of the person

A rate of the reliability of the match is also recorded, enabling to be stricter about the level of accuracy expected. In figure 13, the facial recognition reliability is of 93% (including information on age and emotions).

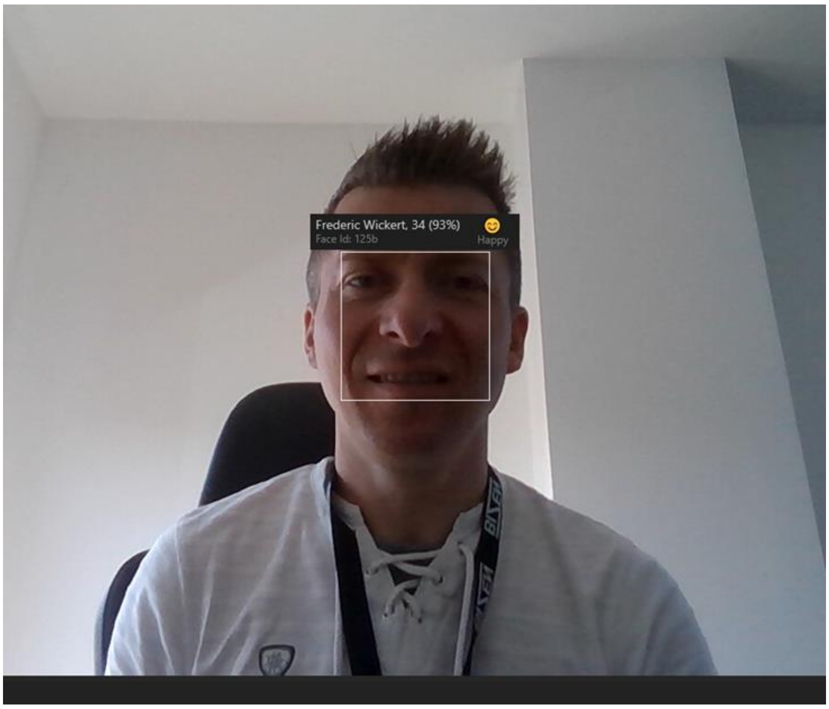


Figure 13: reliability rate of the facial recognition

7. CAMERA

The quality of the match depends on the input photo. In this scenario, the input photo is produced by a camera and sent to the identification service. As a result, the quality of the camera plays a crucial role.

Today’s conventional cameras are high quality devices, but they make no difference between a real face and photo on paper or a smartphone. This makes it easy to pass oneself off as another person. The solution to this problem is an infra-red camera. It makes for better quality even in poor light and does not register faces in photos.

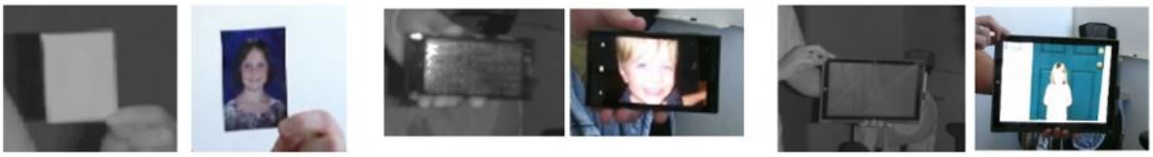


Figure 6: An infra-red camera does not register photos of faces

Apple FaceID and Windows Hello use infra-red cameras.

8. BIASES

It is likely that an algorithm does not detect a face, is wrong about gender, emotion or other skewed analyses by "cognitive" biases.

The biases that can be found in face detection and identification stem from:

- the training photos:
  - an insufficient number of photos;
  - photos not correctly tagged with the right responses: faces not properly framed, humans are also possible of assigning a wrong gender;
  - or identification, photos that are too old confuse the algorithms.
- the quality of the photo sent for detection;
- a poor-quality camera.

9. POTENTIAL USES

These technologies have many uses but they are not all ethical. Here is a list of potential uses:

- enabling visually impaired persons to gain some information about people they encounter with the help of photos coupled with audio feed-back (gender, age, emotion). Example Seeing AI : https://www.microsoft.com/en-us/ai/seeing-ai
- recovering missing children. https://timesofindia.indiatimes.com/city/delhi/delhi-facial-recognition-system-helps-trace-3000-missing-children-in-4-days/articleshow/63870129.cms
- ageing simulation algorithms would make it possible to recognise persons who disappeared when they were children and are now adults. Example FaceApp : https://www.faceapp.com/
- identifying rare genetic diseases: : https://www.genome.gov/news/news-release/Facial-recognition-software-helps-diagnose-rare-genetic-disease
- identifying patients who have got lost in a hospital
- detecting intruders
- supervising individuals' emotions
- determining sexual orientation from facial features https://psyarxiv.com/hv28a/
- determining whether a person is about to commit a crime from their facial features
- detecting emotions during a film, a video game or a show.

And we could imagine many other scenarios.

LEGAL ASPECTS

By Sandra AZRIA, advocate

Introduction

Nothing is more private than one's own body. In the 18th century, the utilitarian philosopher, Jeremy Bentham, devised a concept for prison architecture called the panopticon, in which gaolers stationed in a central tower would be able to supervise prisoners' every action and gesture without being visible themselves. The idea was that the inmates, who could not know whether they were being observed or not, would be forced into a permanent state of passivity. Bentham asserted that the principle could be extended to factories, schools and hospitals. Two centuries later, Michel Foucault argued in his book "Discipline and Punish" that this form of visibility structured around an all-seeing and imperious form of scrutiny was at the core of what he called the modern disciplinary model.

I – CURRENT SITUATION

The current technology – which is imperfect but improving rapidly – is based on algorithms which learn to recognise human faces and the hundreds of ways in which they are all unique.

To do this properly, algorithms must be supplied with hundreds of thousands of pictures of different faces. Increasingly, these photos come from the Internet, where they are scanned by millions of machines unbeknown to those who published them, sorted by age, sex, skin colour and dozens of other parameters, and shared with university research workers or businesses.

For many of us, facial recognition has passed swiftly from the status of a technological novelty to an inescapable day-to-day reality as millions of people are prepared to agree at least to having their face scanned by an airport computer, to pay for a meal[9] or by Facebook's servers.

In Russia, the Central Bank has been conducting a biometric programme since 2017, collecting people's faces, voices, iris scans and fingerprints throughout the country.[10] In India, facial recognition is now used as one of the means of authentication via AADHAAR (the national identification system, which already covers over 960 million people).[11]

A study conducted in 2016 by Georgetown University showed that one American adult in two, which is 117 million people, can be found on a facial recognition database, and there are few rules governing access to such systems.[12]

In any case, there is no doubt that facial recognition technology can be a powerful tool.

1) Increasingly widespread use

The most common uses to date are as follows:

- **Security**: identity documents, border control, police checks and criminal investigations (facial recognition is reported to have helped identify the suspect in the murder of five employees at the Annapolis Capital Gazette on 28 June 2018).[13]

[9] https://www.reuters.com/article/us-alibaba-payments-facialrecognition/just-smile-in-kfc-china-store-diners-have-new-way-to-pay-idUSKCN1BC4EL

[10] https://financialobserver.eu/cse-and-cis/russian-banks-to-use-biometric-data/

[11] https://timesofindia.indiatimes.com/india/face-recognition-to-be-must-for-all-aadhaar-authentications/articleshow/65522828.cms

[12]https://www.law.georgetown.edu/news/half-of-all-american-adults-are-in-a-police-face-recognition-database-new-report-finds/

[13] https://www.theatlantic.com/technology/archive/2018/06/capital-gazette-shooting-face-recognition/564185/

According to a study in 2018,[14] 77% of airports and 71% of airline companies plan to invest in biometric identification technologies in the next three years. And 59% of airports and 63% of airlines are planning in particular to install facial recognition at boarding gates.

The world leader in these technologies is a European company based in Geneva, the *Société internationale de télécommunication aéronautique*, more commonly known by its acronym, SITA. At Roissy-Charles De Gaulle and Lyon-Saint-Exupéry airports, facial recognition has helped considerably reduce border delays[15] as the new gates can link passengers' faces to the photo on their passport. This has made it possible to increase the percentage of passengers eligible for these types of control although the system is still far from perfect. "The obstacles are not technological ones but administrative ones" says the Director of SITA. "European governments need to agree on common standards and regulations need to be harmonised". Some countries such as Australia aim to use facial recognition to automate 90% of passenger checks by 2020.

Lastly, facial recognition systems can help to reunite lost or abducted children with their families and thwart human trafficking.[16]

- **Health**: monitoring patient medicine consumption,[17] detecting genetic diseases[18] (such as DiGeorge syndrome, for which there is a success rate of 96.6%[19]) or supporting pain relief measures.[20]

- **Retail**: uses are growing, particularly to track and analyse customer habits in shops[21] but also to make payments.[22]

  In Australia, Coca-Cola has been testing technology since the beginning of this year on about fifty drinks vending machines capable of relaying advertising messages, collecting sales data and analysing users' interaction through a digital screen and a camera. According to Coca Cola, these distributors have resulted in a 12% sales increase during the test period.[23]

  In the United Kingdom, Tesco has fitted 450 of its service stations with advertising screens delivering advertising in real time according to the age and sex detected by the system's cameras.[24]

  In 2014, Ford and Intel announced the **Mobii** project (PDF), which includes a driver recognition system to personalise driving experience (unlocking, uploading individual settings, incorporating the driver's diary into the GPS system, anti-sleep alarms).[25]

[14] https://www.sita.aero/resources/type/surveys-reports/air-transport-it-insights-2018
[15] https://www.tourmag.com/Aeroports-vers-la-fin-des-cartes-d-embarquement_a97696.html
[16] https://www.telegraph.co.uk/peoples-daily-online/science/china-facial-recognition-missing-persons/
[17] https://journal.ahima.org/2018/09/04/facial-recognition-enters-into-healthcare/
[18] https://ai-med.io/facial-recognition-and-medicine/
[19] https://www.genome.gov/news/news-release/Facial-recognition-software-helps-diagnose-rare-genetic-disease
[20] https://www.sciencedirect.com/science/article/pii/S1877050916300874
[21] https://www.theguardian.com/cities/2016/mar/03/revealed-facial-recognition-software-infiltrating-cities-saks-toronto
[22] http://www.globaltimes.cn/content/1159070.shtml
[23] https://www.businessinsider.com.au/coca-cola-is-using-facial-recognition-technology-on-fridges-in-australia-to-sell-more-drinks-2014-5
[24] https://www.retaildetail.eu/en/news/algemeen/tesco-installing-facial-recognition-camera%E2%80%99s-advertisers
[25] https://thenewswheel.com/project-mobii-facial-recognition/

Every day new uses of this tool are highlighted in the news, along with numerous scandals which raise questions about how possible it is to protect human rights effectively when a facial recognition system is being used.

II - RISKS

1) Privacy

The latest scandal provides a perfect illustration of the potential major impact on the privacy of the data subjects. In August 2019, the UK's supervisory authority, the Information Commissioner's Office (ICO) opened an inquiry on a surveillance system using facial recognition set up in King's Cross, London.[26] Elizabeth Denham, Information Commissioner emphasised in her statement that "scanning people's faces as they lawfully go about their daily lives, in order to identify them, is a potential threat to privacy that should concern us all. That is especially the case if it is done without people's knowledge or understanding".

One of the chief problems posed by facial recognition is that data subjects do not necessarily know that it is being used on them. The number of faces to be processed and the speed of processing required also makes it difficult to apply consent as a legal basis to this processing of personal data (when it is actually applicable), particularly in view of the fact that where sensitive data are concerned, explicit consent should be required.

In addition, access to social networks (whether authorised or not and public or not) affords access to billions of photos that may be used without the consent of the data subjects.

Lastly, in the long term, technological interoperability may have the practical effect that certain types of biometric data will be used as a standard single identifier. An aggravating factor could be that unlike personal identification numbers, which can be changed during one's lifetime, such changes are clearly not feasible where it comes to people's biometric data and still less to their faces.

There is also reason for particular concern about affect recognition, a subclass of facial recognition that claims to detect things such as personality, inner feelings, mental health and 'worker engagement' based on images or videos of faces.

If this is bad, the prospect of the police using affect recognition to deduce what your future criminal activity will be on the basis of your face's "microexpressions" is infinitely worse and thrusts us into the kind of future imagined in the film Minority Report.

In 2016, students at the University of Shanghai published a detailed report on what they claimed was a learning machine method programmed to determine people's criminal potential based solely on their facial features.[27] Their publication was criticised widely for embodying a revival of physiognomist ideas through affect recognition applications.

The idea that artificial intelligence systems might be able to tell us what a student, a customer or a criminal suspect is really feeling, or even what type of person they are deep down, is proving very attractive to corporations and governments, although the scientific grounds for such assertions are highly questionable and we have well-documented accounts of how they have been used for discriminatory purposes.

Whether it is through Faception, which claims to be able to "detect" if a person is a terrorist by surveying their face,[28] or HireVue, which uses mass video recording of candidates at job interviews to predict from their microexpressions whether they will make good employees or not,[29] the ability to use analysis of mass data to make correlations gives rise to very suspect assertions.

[26] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/08/statement-live-facial-recognition-technology-in-kings-cross/

[27] "Automated Inference on Criminality using Face Images", Shanghai Jiao Tong University, 21 November 2016.

[28]https://www.faception.com/

[29] https://www.hirevue.com/blog/7-things-you-need-to-know-about-game-based-cognitive-assessments

In a similar fashion, the authorities in the north-eastern Chinese province of Jilin have decided to crack down on drink driving and the police here have announced that they are going to experiment with new technology to recognise whether drivers are drunk or not.

Several facial features have been singled out to help the technology to determine whether motorists have consumed alcohol. Artificial intelligence will then assess whether there any red patches on their face or whether they are breathless, yawning or hiccupping.[30] When suspect conduct is identified, information will be sent to the nearest police patrols, who will intercept the driver to carry out more detailed tests.

Added to all these risks is the threat that ultimately our anonymity will be completely lost as these tools become available to the general public. It will soon be possible to identify anyone you pass in the street using applications like NameTag or Facezam. Although the latter have proved to be hoaxes, accelerating technological development will almost certainly make this kind of tool a reality soon. The idea was that users running these applications on a smartphone or Google Glass would only have to take a photo of a person to link up to their virtual profiles on social networks and hence to access information on their identity, address, family members, occupation, tastes, etc.[31]

On the other hand, being recognised by a facial recognition system which uses your Facebook photos when you enter a commercial outlet is already possible. The notion seems frightening, even if it was devised to reward customer loyalty. The idea arose at a new advertising agency, based in Nashville in the United States. This agency, Redpepper, is currently testing a camera linking up your Facebook photos to a facial recognition system, the aim being to offer discounts to the customers of small commercial outlets.[32]

For its first use, the camera, dubbed Facedeals, was installed at the entrance to a bar. As customers approach, the camera, connected to Wi-Fi, analyses its targets in order to find their Facebook account. Once they have been identified, Facedeals uses their likes and behaviour on the social network to calculate special offers and reductions, for which they receive a coupon on their mobile phone.

Even if we are particularly careful about the use of our photos on social networks, this technology is so powerful that our anonymity will still be under threat. For example, an incident which seems to be quite charming happened to a Mr Fred B. In 2014 he received an e-mail from Facebook informing him that it had detected his face in a number of photos and asking him if he would like to be tagged in them. When he clicked on the link, he was amused to find eleven black and white headshots of his mother when she was at university. Her face had been wrongly identified as his by the social network's DeepFace algorithm.

According to David Tunnell, the chief technology officer at NXT-ID specialising in three-dimensional facial recognition, "you can use facial recognition to identify a person's ethnicity, region of origin, and family affiliation. With good data from my parents, siblings, or cousins, it might be possible to identify a person even if the system has no actual images of them to work from".[33]

2) Risks linked to the degree of reliability

Despite the remarkable growth in this technology, many questions remain about its reliability and the many threats posed by potential errors.

The use of a system based on biometric data relies inevitably on statistical probabilities. There is no such thing as an infallible system. If there is a sufficient degree of probability, the data subject will be "recognised" by the system.

[30] http://www.xinhuanet.com/english/2019-03/07/c_137875388.htm

[31] https://www.entrepreneur.com/article/290742 « people can't stalk your profile through face recognition apps - Yet »

[32] https://www.adweek.com/digital/redpepper-facedeals/

[33] https://www.theverge.com/2014/9/10/6126027/facebook-is-convinced-this-man-is-his-mother-deep-face

Biometric systems therefore are inherently fallible. The risk of a false match or non-match can have unfortunate consequences for data subjects.

For example, if they are wrongly "recognised" as appearing on a list of wanted criminals, the practical consequence could be that they will have to prove their innocence. The rate of false matches and non-matches depends on several attributes of the system used, such as its quality and reliability, enrolment processes, etc. Rates can be adjusted so as to reach the security level required for the purpose of the system. Efforts to prevent false outcomes should be proportionate to this purpose.

ACLU, the American Civil Liberties Union, has asked Amazon to stop marketing its Rekognition system following a test that highlighted its failings. In this test, the system wrongly identified 28 Congress members as criminals currently serving prison sentences and the false matches were disproportionately of black persons or people of colour.[34]

In London, when the police started testing their own facial recognition system, in 98% of cases in which the artificial intelligence system issued suspect identification alerts, they were false positives. This has given rise to public concerns about the system. Today the error rate is still 81%, which seems astounding in view of the potentially harmful effects for the data subjects.[35]

3) Data security risks

Having said this, the consequences of a breach of the security of facial recognition data are potentially more serious and long-lasting than those of any other kind of personal data breach as it is much more difficult for a person to change their face than it is for them to change their credit card number.

As a result, the news is full of examples of major technical failings in the security sphere.

One such example is the facial recognition function on the Samsung Galaxy S10, which is clearly just as poor as on previous versions as it would seem that it is possible to unlock access to it using a photograph or a video of the owner.[36]

Lewis Hilsenteger has demonstrated the problem on his Unbox Therapy channel on YouTube. By playing a video in front of the smartphone sensor, he was able to deceive the facial recognition system and unlock access to the phone.

An Italian journalist on SmartWorld.it was also able to unlock a Galaxy S10 using nothing but a photo, which seems on the face of it much simpler for a hacker to obtain. However, Samsung and its Galaxy Ss are not isolated cases.

A survey carried out last year by a Dutch association revealed that the unlocking functions based on facial recognition of 42 of the 110 smartphones it tested could be tricked using nothing but a photo.[37]

4) Freedom of expression and freedom of religion

The most virulent criticism of facial recognition is, of course, prompted by these most serious breaches, particularly those linked to freedom of expression and religion.

Civil liberties campaigners fear increasingly that the police may deploy facial recognition in "real time" using drones, body cameras and vehicle dash cameras.

[34] https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28

[35] https://www.technologyreview.com/f/613922/london-polices-face-recognition-system-gets-it-wrong-81-of-the-time/

[36] https://www.zdnet.com/article/samsung-galaxy-s10-facial-recognition-fooled-by-a-video-of-the-phone-owner/

[37] https://www.zdnet.com/article/facial-recognition-doesnt-work-as-intended-on-42-of-110-tested-smartphones/

"The real concern is police on patrol identifying law-abiding Americans at will with body cameras", says Matthew Feeney, a specialist on emerging technologies working for the libertarian think tank, the Cato Institute.[38]

An even more worrying situation is playing out in the province of Xinjiang in China (where there is a large Muslim community of Uighur origin).

All citizens of this province over the age of 12 must have their face scanned in 3D to facilitate the work of facial recognition cameras. This mass surveillance – whose official aim is to prevent terrorism – helps the authorities to identify all types of conduct that they regard as "extremist", such as travelling more than 300 metres from one's home, going to the mosque too often or even filling up at the petrol station several times a week.[39] "Persons who are caught run the risk of being sent to a re-education camp", says Maya Wang. It is reported that a million Uighurs are already interned in such camps.[40]

5) Freedom of movement

Many experts also highlight the potentially crippling effects on freedom of expression, action and association and other civil rights caused by the loss of anonymity resulting from constant public surveillance by facial recognition systems.

There is particular cause for concern in the government surveillance field. Facial recognition tools devised for military uses abroad are applied increasingly for law enforcement purposes in the United States, with few guidelines and little public scrutiny.

For instance, a document published by the American Department of Homeland Security highlighted by the ACLU shows that the White House plans to set up a facial recognition system enabling it to identify and follow the movements of potentially dangerous individuals.

The system is still at the test stage but poses major risks of abuse. Without being able to do anything to stop it, passers-by walking in the vicinity of the White House in Washington could soon have their faces recorded and analysed by the US secret services.[41]

The upshot is that several thousands of persons – whether activists, tourists or government officials – would be scrutinised in this area of Washington without their consent.

This is a problem which the document sweeps aside in one somewhat flippant sentence: "Individuals who do not wish to be captured by … cameras involved in this pilot may choose to avoid the area", clearly showing how the principle of freedom of movement is being undermined.

If it is successful, the system could make it possible for officers in charge of White House security to track the movements of persons whom the document refers to as "subjects of interest".

The question is what criteria will be used to decide that a passer-by is a "subject of interest" and in the ACLU's opinion, this is precisely where the problem lies. "We don't exactly know how the Secret Service determines if someone is a 'subject of interest'", says one of the ACLU's members, Jay Stanley, in an article on its site. "The agency says they could be flagged through a variety of means, including 'social media posts made in public forums' as well as suspicious activity reports and media reporting. Unfortunately, our government agencies have a long history of labelling people threats based on their race, religion, or political beliefs. Just last year, for example, a leaked document revealed that the FBI had prepared an intelligence assessment wrongly profiling Black activists as threats based on their race and beliefs, labelling them 'Black Identity Extremists'".

[38] https://fee.org/articles/should-police-be-able-to-use-facial-recognition-technology/

[39] https://www.theguardian.com/world/2018/jan/18/china-testing-facial-recognition-surveillance-system-in-xinjiang-report

[40] https://www.lemonde.fr/asie-pacifique/article/2018/08/31/la-chine-detiendrait-un-million-d-ouigours-dans-des-camps-d-internement_5348573_3216.html

[41] https://www.aclu.org/blog/privacy-technology/surveillance-technologies/secret-service-announces-test-face-recognition

In a lighter vein, although just as noteworthy, Mike Downing, chief security officer at the Oak View Group, who took the opportunity to test facial recognition at a Taylor Swift concert, explained how it worked to Rolling Stone magazine: “Everybody who went by would stop and stare at it [a screen playing rehearsal clips with an embedded camera], and the software would start working”.

The recorded images were sent immediately to a command post in Nashville, Tennessee, which cross-referenced them with a database of about one hundred persons who had already been found to have been stalking the singer. This use of the technology inevitably raises questions concerning respect for privacy.[42]

The current justification for the use of the system is security at shows, but in future it could be used for other reasons. The group TicketMaster has stated that it aims ultimately to replace conventional tickets and e-tickets with face scanners so that spectators can enter events more quickly and easily. For this purpose, the group has already invested in the start-up Blink Identity, whose sensors can identify a person walking by them in half a second.[43]

6) Risks of discrimination

Several studies have demonstrated the high risks of discrimination on the ground of skin colour or gender associated with facial recognition.

For instance, a study published in July 2019 by the National Institute of Standards and Technology (NIST) of the US Department of Commerce[44] revealed that facial recognition algorithms made ten times more errors concerning black people and, more particularly, where it came to women.

The latest cause for concern is a study published by MIT’s Media Lab,[45] in which it was revealed that Rekognition yielded poorer results when trying to identify a person’s sex if that person was a woman or had darker skin.

In tests conducted by Joy Buolamwini from MIT, Rekognition made no mistakes when attempting to identify the sex of men with light skin but it confused women with men 19% of the time and women with darker skin with men in 31% of cases.

Another study by Buolamwini on a tool developed by Microsoft, IBM and MEGVII highlighted similar errors.[46]

Microsoft announced last month that it had made significant improvements to facial recognition across skin tones and genders.

IBM has stated that it was launching a major study to “improve the understanding of bias in facial analysis”.[47]

Lastly, we cannot overlook the fact that Google’s photo service still censors the search terms “gorilla” and “monkey” after an incident in 2015 in which algorithms labelled black people gorillas.[48]

7) Access to and control over data

In this sphere as well, it regularly emerges that personal data linked to facial recognition are shared and disseminated without the data subjects even being informed.

[42] https://www.rollingstone.com/music/music-news/taylor-swift-facial-recognition-concerts-768741/

[43] https://www.theverge.com/2018/5/7/17329196/ticketmaster-facial-recognition-tickets-investment-blink-identity

[44] “Ongoing Face recognition – vendor test”, National Institute of Standards and Technology, 22 July 2019

[45] “Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products”, Association for the Advancement of Artificial Intelligence, 25 January 2019.

[46] https://www.theverge.com/2018/2/11/17001218/facial-recognition-software-accuracy-technology-mit-white-men-black-women-error

[47] https://www.cnbc.com/2019/01/29/ibm-releases-diverse-dataset-to-fight-facial-recognition-bias.html

[48] https://www.theguardian.com/technology/2018/jan/12/google-racism-ban-gorilla-black-people

Yet, even if people succeed in identifying the commercial bodies which have collected data on them using facial recognition systems, it may be difficult or impossible for them to determine what data have been collected, how they have been used and with whom they have been shared, and then to gain access to them so as to correct errors or remove information concerning them.

In January 2019, IBM used and shared a gallery of some one million photos that it had collected from the photo-hosting site Flickr to describe the appearance of the subjects and train its facial recognition tool. IBM conducted an extensive communication campaign on this process targeting researchers and presenting it as a progressive step designed to reduce bias in facial recognition.[49]

However, it soon became clear that these photos had been shared and disseminated without the consent or even the knowledge of the data subjects.

In response IBM simply gave an assurance that Flickr users could ask to be withdrawn from the database. In practice it has proved almost impossible to have photos removed.

IBM required photographers to send links by e-mail to the photos they wished to remove, but the company has not shared the list of Flickr users and photos included in the dataset publicly. As a result, there is no way of determining who owns the photos that were included, and the data subjects are deprived of any real rights in this respect.

[49] https://www.theverge.com/2019/3/12/18262646/ibm-didnt-inform-people-when-it-used-their-flickr-photos-for-facial-recognition-training

RECOMMENDATIONS

Facial recognition technology is making rapid progress and the algorithms are increasingly effective. However, certain biases persist and there is no guarantee that new ones will not arise. Furthermore, it is not the tool that might be called into question but rather the manner in which it is used. This is why a number of technical recommendations are needed to enable everyone to set up and use facial recognition within a responsible, transparent and ethical setting.

It is necessary to think about what recommendations should be made to move current facial recognition practices towards increased respect for human rights protection.

Convention 108+ is the only existing international treaty which guarantees individuals the right to protection of their personal data, its aim being to prevent any abuse which may arise when such data is processed. It was opened for signature by any country and is the only binding legal instrument with the potential to be applied throughout the world, thus offering legal certainty and foreseeability in international relations in the field.

The principles laid down in Convention 108+ can be used to improve the protection of persons when they are faced with the use of facial recognition systems.

It is worth noting that several big players in the creation of facial recognition technology have raised questions about the risks posed by this technology. [50]

Each recommendation detailed below will be structured by specifying the subject of the recommendation and the stakeholders involved. The actors will be categorised into:

- **Editors, Developers and Integrators:** Any person, natural or legal, who develops or deploys facial recognition models.
- **Decision-makers and Legislators:** Any person, natural or legal, who is responsible for the uses resulting from a facial recognition system.
- **Users:** Anyone whose personal data is being used by facial recognition applications.

I.1 Legal basis

The question of the legal basis enabling the processing of personal data in the context of facial recognition technologies is of a crucial importance.

[50] In June 2018, Microsoft launched an appeal for regulation by the authorities and private enterprise: https://blogs.microsoft.com/on-the-issues/2018/07/13/facial-recognition-technology-the-need-for-public-regulation-and-corporate-responsibility/

In December 2018, Microsoft incorporated 6 governance principles into its facial recognition technology.

These are as follows:

- fairness
- transparency
- accountability
- non-discrimination
- notice and consent
- lawful surveillance

Details of these principles can be consulted here: https://1gew6o3qn6vx9kp3s42ge0y1-wpengine.netdna-ssl.com/wp-content/uploads/prod/sites/5/2018/12/MSFT-Principles-on-Facial-Recognition.pdf

This is a first step, which can be welcomed.

Basing the processing on consent should not be the rule but the exception, furthermore underlining the strict conditions of validity of consent, which being biometric data are sensitive data, requiring that consent be given explicitly.

One of the main factors to be taken into account when collecting facial recognition data from a potentially large number of people is if and how their informed consent is to be obtained, particularly if these persons are subsequently to be identified or profiled in relation to other sets of data.

The problem is that data subjects may be unable to meaningfully give or withdraw consent to the collection of facial recognition data given that these systems are used increasingly in public places.

Entities using facial recognition technologies will therefore need to respect the following recommendations:

- take measures to obtain explicit and affirmative consent, particularly before identifying an anonymous or unidentified person and, of course, when this identification is passed on to third parties which were not already aware of their identity outside the context of the relationship with the data subject.
- If this is not possible, to seek ways of minimising the use or impact of facial recognition technologies on data subjects and to undertake to collect, use and share such data in a way that is compatible with the context in which they were collected, taking into account the probable impact on persons and the potential benefits to individuals of ground-breaking uses of data.
- ensure that consent is given freely, there is also a need to propose alternative solutions to data subjects (such as passwords or swipe card devices). It is also essential to see to it that such solutions are easy to use as, if they are too long or complex compared to facial recognition, there will be no real choice.
- If consent is given for one purpose, data should not be used for another purpose without consent. Similarly, if data is transmitted to a third party, this transfer should also be subject to specific consent.
- Any information given before data are collected must of course meet the transparency requirements referred to hereafter to ensure the quality of the consent.
- No standard biometric identifier should be created and kept over time without appropriate consent.
- For minors, verifiable parental consent must be given.
- Lastly, withdrawal of consent must be catered for at technical level to ensure that it is effective.

I.2 Limitations of use - Proportionality

Companies should also examine how the use of facial recognition technology will affect both those who use this technology deliberately and those who enter into contact with facial recognition products or services accidentally or cannot reasonably avoid a facial recognition system being used by a company.

For example, where facial recognition data are used to try to match a person’s faceprint with a series of reference data from registered users, companies should attempt to delete all the data from the facial recognition programme where no match has been found.

The choice between a verification system and an identification tool depends largely on the planned purpose of the facial recognition system and the circumstances in which it will be used. The tool therefore must serve the purpose for which the data were collected and not be unnecessarily oversized. For instance, opting for an identification system when a verification system also seems possible will call for special justification.

In addition, one of the unusual features of the biometric data connected with facial recognition is that they often contain more information than is necessary for verification or identification. It is possible to avoid excessive data processing by limiting the storage and use of data. The system should therefore be devised in such a way that the data obtained only reveal the information needed for its purpose. In particular, it should avoid the possibility of any link being made with other sensitive data (for instance, an illness).

Personal data should not be processed later in a way that the data subject may consider unexpected, inappropriate or reprehensible.

Furthermore, where data are transferred to third parties or disseminated in public (particularly on social networks), technical and/or legal means of preventing uses other than those initially planned need to be identified. These measures may include technical means of making individual images unrecognisable, restrictions on automated access to the relevant databases and contractual obligations requiring partners to respect the legal framework.

Despite the safeguards made possible by the legal armoury that can be applied to facial recognition, particularly Convention 108+, it seems clear that in some cases its use should be strictly limited or even prohibited by national legislation.[51]

Thus, facial recognition should never be used to determine a person's colour, religion, sex, origin, age or state of health (except, of course, as part of a medical research project).

Similarly, affect recognition is a subcategory of facial recognition which claims to detect things such as personality, inner feelings, mental health and 'worker engagement' based on images or videos of faces. As these claims are not supported by sound scientific evidence, there is a risk that they will be applied in an unethical way. Establishing links between affect recognition and decisions on hiring, access to insurance, education and police services give rise to very alarming risks affecting both individuals and society as a whole and could therefore be prohibited.

At any rate, it is essential to ensure at least that the use made of this tool is proportionate and shows due regard for its purpose and its impact on the rights of data subjects.

cannot be a judge of the ethical standards of the various types of use, but they do need to be categorised and it is essential for there to be some form of a framework for facial recognition, which would determine, depending on the use being contemplated:

- the content of a detailed explanation of the use in question, the purpose sought;
- the minimum reliability of the algorithm: minimum reliability rate;
- the length of storage of the photos used for identification;
- the possibility of auditing these criteria;
- the traceability of the process, secured by means of a blockchain for example.

Editors, Developers and Integrators: Editors providing pre-trained templates cannot guarantee the use of their algorithms, but can still have developers using their solution sign an ethical charter. On the other hand, the latter must specify in which category the use they make of them will be classified.

Decision-makers and Legislators: This framework is fundamental to better manage the use of facial recognition. It is imperative to formulate this framework.

I.3 Transparency

One of the greatest risks posed by the use of facial recognition is that, unlike other biometric data, it can be used completely unbeknown to the data subject, as demonstrated by the information revealed very recently on the surveillance system set up at Kings Cross in London and the investigation on this carried out by the Information Commissioner's Office (ICO).[52]

[51] See, on this point, the statement by Clare Garvie, Senior Associate on Privacy and Technology at Georgetown Law at the hearing on "Facial recognition technology: its impact on our civil rights and liberties". She calls in particular for an outright prohibition on the use of driving licence photos in criminal investigations and for use in general to be limited to investigating violent crimes.

[52] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/08/statement-live-facial-recognition-technology-in-kings-cross/

It is essential therefore to make such use subject to real and effective transparency (Article 5, Convention 108+).

Factors which will determine whether use is compatible with the principle of transparency include the information provided for people, the context in which the data were collected, reasonable expectations as to how they will be used, whether facial recognition is just one of the features of a product or a service and not an integral of the service itself and how the collection, use and sharing of facial recognition data is likely to impact people, particularly when it is used on minors or children under 13 years of age or persons in a vulnerable situation.

It is furthermore important to establish a form of transparency which gives everyone a clear and understandable overview of the technology and its use, while duly respecting professional confidentiality.

The first step towards making a facial recognition process "transparent" is to produce educational material (such as articles, images, videos and FAQS) on the data, how the algorithm functions, the process and its reliability.

More broadly speaking, for the public to understand more about artificial intelligence (and facial recognition in particular), they need to be educated.[53] People need to be alerted to the issues at stake and rendered more digitally literate (What happens when you post something on the social networks, when you upload a video or when you click on an advert?[54]).

There is a need therefore to set up an education programme to raise awareness among as many people as possible, whether school pupils, professionals, pensioners or others.

- Privacy policies in relation to facial recognition or information material should include the following information[55]:

    - purposes for which facial recognition data are collected;
    - whether facial recognition data may be shared;
    - retention, deletion, or de-identification policies for facial recognition data;
    - choices data subjects may have regarding their facial recognition data;
    - where data subjects may direct questions about their facial recognition data;
    - what contracted third party partners routinely receive the data as part of supplying the product or service;
    - when collection, use, and sharing practices materially change, companies should update their public privacy policies or publicise those changes as appropriate to the context of the change and its impact on data subjects.

- **Editors, Developers and Integrators:**

    They should seek to take reasonable steps – such as providing guidance and advice on how to facilitate transparency and privacy compliance by third-parties using their facial recognition technology, notably by :

    - including reasonable limitations on use in the terms of the contract;
    - providing companies with model language for physical location signage or inclusion in their privacy notices;
    - recommending signage if the facial recognition technology will be deployed in public places; and,
    - recommending other reasonable efforts to promote provision of clear, meaningful notice to users.

[53] As proposed by Finland https://www.technologyreview.com/f/612762/a-countrys-ambitious-plan-to-teach-anyone-the-basics-of-ai/.

[54] In terms of artificial intelligence and data collection

[55] See, in this connection, the recommendations of the Future of Privacy Forum "Privacy Principles for Facial Recognition Technology in Commercial Applications" https://fpf.org/2018/09/20/fpf-releases-understanding-facial-detection-characterization-and-recognition-technologies-and-privacy-principles-for-facial-recognition-technology-in-commercial-applications/

They could furthermore set up user training, videos and tutorials explaining how the technology and system work before using them.

- **Decision-makers and Legislators:** They could set up an educational programme (national or in the company depending on the context of use) to raise awareness among users.

  With regard to the public sector, which is now very involved in the use of facial recognition, it would be useful for public procurement procedures to include specific rules on transparency and prior assessment of the facial recognition system providers.

- **Users:** They could follow a tutorial with an assessment of prior learning to ensure that they are aware of the use and implications of facial recognition.

I.4 Quality of data

Like other applicable regulations, particularly the GDPR (General Data Protection Regulation), Article 5 of Convention 108+ includes a requirement with regard to accuracy for data. This point is key to facial recognition because it has been proved repeatedly that errors are frequent and have major consequences for the data subjects (see part 1).

Accordingly, both designers and users should take steps to ensure that facial recognition data are accurate and, in particular, to prevent labelling errors by testing their systems sufficiently to identify and eliminate significant disparities in accuracy, especially with regard to demographic variations of colour, age and sex, and hence to avoid all unintended discrimination.

On another level, a response needs to be found to questions raised by persons with disabilities and persons whose physical characteristics do not correspond to the technical standards of the tool used. Back-up procedures need to be provided for in case the system fails in such circumstances.

Furthermore, the collection of personal data in preparation for automated processing poses a further problem if these biometric data inevitably but unnecessarily reveal other sensitive data such as information on a type of illness or physical disability.

I.5 Quality and training of algorithms

The first step is for algorithms to be trained to recognise faces in a photo. To achieve this, labelled photos are used (with replies – see section on “General functioning”).

I.5.1 Photo diversity

To take account of all the features of different faces, a data set that represents the entire population is recommended, in other words a series of varied photos including:

- women
- men
- varying skin tones
- varying morphologies
- all ages
- photos from various angles.

However, it is pointless to require a minimum number of photos. It is actually the degree of diversity that needs to be quantified. One could imagine a line of research whose goal would be to perfect a facial recognition algorithm which would need fewer photos than today[56].

Photo diversity is therefore essential to prevent certain biases and to make algorithms more reliable.

[56] It means here to train the algorithm to find out the presence of faces and not to recognise a particular face, which, as we already saw, does not require many photos.

Editors, Developers and Integrators: They could specify factually the diversity of the photos used. How many photos of this or that type are used for a particular version of the algorithm?

Decision-makers and Legislators: They could provide a minimum framework for photo diversity.

Users: They should have the opportunity to consult this information easily.

I.5.2 The life span of data sets

For a person to be recognised, training data (the photos of faces to be recognised) should not be too old. They should be regularly updated. It is impossible to set a fixed deadline for such updates (5 or 10 years) – it would make no sense to do so.

On the other hand, as it has been pointed out, every algorithm yields a rate of reliability of matches. This percentage needs to be historicised and the system becomes less reliable over time, the training photos need to be updated, meaning that users need to be asked again for more recent photos.

It could be recommended for instance that if the reliability rate falls by 10% or more over two years, the system should ask for more recent photos. However, if the drop-in reliability is a general trend affecting all matches, it is the algorithm itself that should be updated.

This will also shield the system from the effects of changes in the forms of faces as a result of ageing, accessories (such as body piercing), accidents altering a part of the face, etc.

These records of reliability rates (of the algorithm as a whole and in relation to specific users) must be easily available to users in the form of scoreboards for instance.

This would also enable users to renew or withdraw their consent to the use of their photos for facial recognition**.**

Editors, Developers and Integrators: They could set up a historical dashboard of the reliability of their algorithm, the age of the photos used for facial recognition (personal and global) that can be easily consulted.

Users: They should have the possibility to consult this information easily and choose to delete all or part of the photos used and to renew such photos.

I.6 Reliability

We have seen that artificial intelligence algorithms are “stochastic” and a reliability rate enables us to know how they are performing.

We can contemplate setting a minimum rate of reliability but in this case, it must depend on the circumstance in which the technology is used. A system to recognise the faces of customers in a store does not necessarily need to be as reliable as a system to recognise ATM users[57] or a system to detect criminal suspects.

Editors, Developers and Integrators: They could set up a historical dashboard of the reliability of their algorithms.

Decision-makers and Legislators: They could provide a framework on minimum reliability depending on the scenario. Different categories will then be required with different requirements. (Non-critical to critical for example)

The use of facial recognition by the public authorities in particular could be subject to minimum performance levels in terms of accuracy, especially where it is used for public order related purposes.

[57] https://news.microsoft.com/en-au/2018/10/23/nab-and-microsoft-leverage-ai-technology-to-build-card-less-atm-concept/

Users: They should have the opportunity to consult this information easily.

I.7 Traceability

Every step of the facial recognition process must be traced. We have the technical means of tracing input data, the reliability of the algorithm, trends in this reliability over time, successive versions of algorithms and so on. The aim should be to make this information available to users using clear language that can be understood by everyone.

However, in a complex neural network, it is impossible to explain exactly why things happen. Why are certain neurons more active and more weighted than others? It is precisely the “learning” in deep learning processes which enable networks to learn to recognise a face without us having to give them detailed information about what a face is. Even if we know that a particular neuron was activated with a particular weighting, nothing explains why. And as things stand it is impossible to know this.

Editors, Developers and Integrators: They could set up a detailed dashboard on the traceability of their algorithms: Data, reliability, versions, etc...

Decision-makers and Legislators: They could provide a framework for minimum traceability.

Users: They should have the opportunity to consult this information easily.

I.8 Security

In light of the sensitive nature of the data processed, any breakdown in data security is likely to have particularly major consequences for data subjects given that unauthorised dissemination cannot be corrected, as would be the case with a password.

There is a need therefore to implement strong security measures to protect facial recognition data and sets of images from loss and from unauthorised access or use during collection, transmission and storage. Reasonable security measures should include data encryption and a combination of anti-virus protection, access controls, employee training and other high-level safety practices.

Security measures should evolve over time and in response to changes in the threats and vulnerabilities identified. They should also be proportionate to the sensitivity of data, the context in which facial recognition technology is used, its purposes, the probability of harm being caused to persons and other relevant factors.

Companies should establish strict practices for the storage and elimination of facial recognition data, making for the shortest possible storage times.

Editors, Developers and Integrators: They will have to set up strong security systems: Data encryption, protection of incoming and outgoing flows, supervision, internal audit.

The specific importance of infrared **cameras**:

As with the reliability of algorithms, camera quality does not have to be the same in all circumstances. For the management of identities, it would be harmful for systems to allow an identification by means of a photo held up in front of the camera. This would make identity theft child’s play.

This is why, where facial recognition is used instead of passwords to open user accounts, it is essential for cameras to be equipped with an infrared lens.

Editors, Developers and Integrators: For an authentication system, it is imperative to use an infrared sensor system or other system to avoid the usurpation of a photo.

I.9 Impact analysis and risk assessment

In accordance with the principle of the legitimacy of data processing set out in Convention 108+ and the obligation to prevent or minimise the impact of data processing on the fundamental rights and freedoms of data subjects, an assessment of the risks of the potential impact of processing is necessary to strike a balance between the protection of these rights and the various interests served by the use of facial recognition.

It is crucial to implement an internal review process designed to identify and alleviate potential risks of infringements of privacy in products and services which use facial recognition technology before these products and services are made available or deployed.

A systematic assessment of existing facial recognition tools, gauging their potential impact on the rights of individuals in the light of the nature, context, scope and aims of the system should be required. These analyses should not of course be limited to identifying risks but also propose effective solutions enabling them to be significantly reduced.

Where a public authority has not yet acquired or developed a facial recognition system, such assessments should be carried out before acquisition and/or development and made public. The authorities should also require all suppliers of the planned tool to lift any restrictions on the exchange of information if this has a limiting effect on the impact analysis.

Such impact analyses may be carried out by an independent supervisory body or by an auditor with the relevant expertise so as to help discover, measure or map out repercussions and risks over time.

Impact analyses should of course be carried out at regular intervals.

If a risk is identified which cannot be limited, the bodies concerned should be able to refer the matter to any ethics committees set up and of course initially to the relevant supervisory authorities in order to investigate the risks posed in the human rights sphere.

Lastly, all these processes should be coupled with a “privacy by design” approach in the implementation of any new project.

I.10 Privacy by design

Systematically integrating ‘by design’ the privacy and data protection considerations and requirements provides a sound guarantee that human rights are being protected.

Editors, Developers and Integrators should implement the principle of privacy by design, including by:

- anticipating and preventing events which infringe human rights and privacy before they occur;
- incorporating the protection of privacy and data protection into the design and architecture of facial recognition products and services and into in-house computing systems and the use of dedicated tools;
- incorporating this approach into their organisational practices including, for example, by assigning dedicated staff to these tasks, training employees in the protection of privacy and conducting analyses of privacy protection when developing or altering facial recognition products and services.

This issue has already been partly addressed by the Council of Europe Guidelines on Big Data, which suggest a by-design approach to avoid “potential hidden data biases and the risk of discrimination or negative impact on the rights and fundamental freedoms of data subjects, in both the collection and analysis stages”.

However, this approach should obviously not just be taken on a technical side. There is a need to involve other professionals in its implementation and, in particular, as recommended in relation to artificial intelligence in the report by Professor Mantelero, to set up “committees of experts in various fields (social sciences, law, ethics, etc.), which may provide the best framework in which to engage in debate and address the question of the impact (of IA) on individuals and society, compensating thereby for the narrow perspective of developers".[58]

On this point, reference can also be made to the specific recommendations to take according to the nature of the body concerned (designer, distributor or user) in Opinion 03/2012 of the Article 29 Working Party on the development of biometric technologies, which is still relevant.

I.11 Quality labelling/Certification

Pre-defined criteria (building upon the present recommendations) should be the subject of a quality labelling or certification system confirming companies' technical capacities to develop such technologies, sense of responsibility and ethical principles when using facial recognition or even artificial intelligence in the broadest sense.

This labelling could be applied at several levels according to the field of application concerned.

Editors, Developers and Integrators - Depending on their actual role, facial recognition designers and integrators should specify:

- what data they use;
- how long the data are kept;
- how diverse these data are;
- known biases and how they are avoided;
- what editor they use;
- whether they are certified;
- whether they have signed an ethical charter;
- what scenarios they set up;
- whether they are trained in and aware of the implications of the technology;
- etc.

Decision-makers and Legislators: they should enable the development of tools of labelling/certification to be applied at several levels according to the field of application of the technology:

- a level to categorise the type of structure involved:
  - algorithm developers;
  - algorithm integrators;
  - etc...
- a level to categorise the type of algorithm:
  - computer vision;
  - language: sentence comprehension and generation;
  - intelligent search;
  - etc…
- A level to categorise use types:
  - critical;
  - non-critical;
  - etc...
- etc.

I.12 Training and education

There is a need, as has already been mentioned, for awareness-raising and training for data subjects in artificial intelligence. The idea is not to train engineers and technicians in artificial intelligence but to provide sufficient knowledge for people:

[58] "*Artificial Intelligence – Challenges and Possible Remedies*". Professor Mantelero, associate professor of private law at the Polytechnic University of Turin.

- to understand what providing their data entails;
- to understand the main lines of how artificial intelligence functions;
- to be able to detect when artificial intelligence is being used;
- to be aware of the potential risks if it is misused (identity theft using a photo and a non-infrared camera, for example);
- etc.

I.13 Ethical frameworks and self-regulation

It seems crucial to provide an ethical framework for the use of this technology. Regulations are essential of course but companies also “need internal accountability structures that go beyond ethics guidelines”.[59] This could also take the form of advice from external ethics consultants capable of carrying out audits and publish the results of their research.

Furthermore, in order to avoid human rights infringements, gatherings of experts from various fields of expertise (see above) would be able to establish which are the most high-risk scenarios when using facial recognition technology.

Whistle-blowers also have a major part to play in this area. Employees of companies or bodies developing or using such tools should be granted appropriate protected status. Their role is regularly highlighted, as was the case for example with the employees of Amazon who teamed up with the American Civil Liberties Union (ACLU) to ask their company to stop selling their facial recognition system.[60]

Editors, Developers and Integrators: Technically, editors can set up a framework for using their facial recognition technology and provide integrators with training, detailed documentation and technical certification on the use of this technology.

Decision-makers and Legislators: They can ensure that they provide an ethical and technical framework for the use of facial recognition.

Training programmes and audit procedures for data controllers using facial recognition should be put in place.

It would also be worth planning to set up internal evaluation committees to assess and approve all forms of processing dealing with data from facial recognition systems.

These principles should be extended to contracts with third-party service providers, commercial partners and companies using facial recognition technologies, meaning that access will be refused to third parties who do not comply with them.

[59] AI NOW 2018 - Report

[60] AI NOW 2018 - Report