OPINION N°8
ETHICAL ISSUES OF FACIAL, POSTURE AND BEHAVIOURAL RECOGNITION TECHNOLOGIES

COMITÉ NATIONAL PILOTE
D'ÉTHIQUE DU NUMÉRIQUE

sous l'égide du
COMITÉ CONSULTATIF NATIONAL D'ÉTHIQUE
POUR LES SCIENCES DE LA VIE ET DE LA SANTÉ

OPINION N°8

ETHICAL ISSUES OF FACIAL, POSTURE AND BEHAVIOURAL RECOGNITION TECHNOLOGIES

THIS OPINION WAS ADOPTED UNANIMOUSLY BY THE MEMBERS DURING THE PLENARY ASSEMBLY OF THE CNPEN ON 20 NOVEMBER 2023

How to cite this opinion:
Ethical issues of facial, posture and behavioural recognition technologies; Opinion 8 of the CNPEN 20 November 2023.

CONTENTS

LIST OF INSETS

FOREWORD

This opinion takes a closer look at the ethical issues surrounding systems that incorporate facial, posture and behavioural recognition technologies. As explained in the report that the CNIL (France's data protection authority) published on the subject[1] in 2019, the use of biometrics in general, and facial, posture and behavioural recognition technologies in particular opens up a wide range of potential applications. Some applications could be beneficial to society as a whole, but others legitimately raise major concerns about their impact on civil liberties. Due to their ambivalent nature, it is neither possible nor desirable to issue a clear-cut opinion about the use of these technologies. For each use case, however, it is important to provide an accurate and thorough assessment as to whether the technologies deployed are justified in light of their expected benefits, while anticipating the consequences of their deployment on society in the short, medium and long term. This opinion focuses on the ethical considerations that should be applied to each specific case. It aims to enlighten, not judge. It does not condemn or seek to promote the use of any given approach. It examines the topic without any preconceived ideas and addresses all the stakeholders involved in the various aspects of implementing these technologies. This includes the designers and researchers pioneering these technologies, the engineers involved in their implementation, the companies manufacturing and marketing the devices, and designing the associated applications, products or services, the decision-makers using these technologies to further a policy, the legislators and institutional representatives with responsibility for defining the framework governing their deployment, and finally the operators and the people exposed who potentially benefit from the technologies, but who also suffer the effects. This opinion endeavours to help the various stakeholders form an accurate opinion that is tailored to each situation, based on tangible arguments and a rigorous approach.

1. INTRODUCTION

The development of facial, posture and behavioural recognition technologies has accelerated at a significant rate over the last decade, both in their design and their use, especially for surveillance purposes, but not exclusively. Systems equipped with these algorithm-driven technologies are capable of automatically detecting people, gestures and behaviour with the aim of identifying, authenticating or categorising people or their actions in both the public and private spheres, whether in real time or after the event. Some systems could potentially be beneficial to society as a whole, while others spark major concerns and fears about civil liberty violations, which gives rise to very clear-cut positions, controversies and dilemmas that need to be objectified.

Through this opinion, the CNPEN wishes to enlighten debates on these aspects by exploring the ethical issues raised by the technologies integrated into facial, posture and behavioural recognition systems. Their applications have multiplied and spread to such an extent that all stakeholders need to consider the merits, drawbacks and even potential dangers of each application according to the context surrounding its use. Facial, posture and behavioural recognition technologies offer a number of conveniences for users. For example, they are increasingly used for proving the user's identity in a wide range of services, whether accessing a bank account remotely, unlocking a smartphone, crossing over a border or cutting down on the number of times that ID papers have to be presented at an airport. They are touted as bringing added value to a given service or application, but their limitations, consequences or conditions are not always specified.

They are sometimes used without people's knowledge or under varying degrees of duress in the form of surveillance, or via individual or collective biometric tracking in public, private or transit spaces. They can also lead to a highly intrusive way of tracking people through detection, monitoring or access control systems, which occasionally use emotion recognition mechanisms or specific biometric data. This also applies to purposes that may involve complying with a law, a private regulation or an objective of public interest, as well as purposes defined by private operators for other types of services. The fact remains that the conditions for designing and using these technologies are rarely explicit, which rekindles fears that society will see the emergence of a Panopticon system which, like Michel Foucault's "faceless gaze", would transform "the whole social body into a field of perception".[2]

Automated facial, behavioural and posture recognition technologies have entered widespread use in our environment and are increasingly presented as a solution in an international context that is tending to generalise or standardise their use.

1. CNIL - Facial recognition, for a debate living up to the challenges, 2019. https://www.cnil.fr/sites/cnil/files/atoms/files/facial-recognition.pdf
2. M. Foucault - *Discipline and Punish: The Birth of the Prison*. Gallimard. 1975.

In the run-up to the 2024 Olympic Games, there are suggestions of using these technologies to detect crowd movements and thereby anticipate bottlenecks and prevent their potentially disastrous consequences, which would ultimately improve collective safety. This system differs fundamentally from the facial recognition technologies that were previously used in 2021 to check athletes, volunteers and staff in the stadiums and facilities of the Tokyo Olympic and Paralympic Games2[3].

These technologies have been increasingly implemented by the security sector for border control operations since automated control mechanisms were introduced, such as the PARAFE system in 2017. They are sometimes combined with pre-existing CCTV systems in towns and cities, public transport (train stations, the underground and airports), leisure and shopping areas, and schools. Police forces use them to resolve specific situations or incidents (thefts, accidents, tracking down missing persons or offenders, etc.). Some local authorities have experimented with controlling access to events or schools. A prime example was the Nice Carnival in 2019. Plans to deploy these technologies in the public space have two distinct, but non-exclusive aims, i.e. a preventive purpose (administrative authorities) to prevent offences or attempt to intervene when they are committed, and a repressive purpose (police) to apprehend the people committing these offences and provide evidence for the subsequent investigation.

Thanks to advances in deep learning, healthcare professionals can analyse emotions and behaviour to detect certain illnesses, such as DiGeorge syndrome3[4], or patients' reaction to pain with the aim of adjusting their treatment accordingly. In the commercial sector, these technologies provide an easier way of tracking consumers and giving customers access to services over the Internet. For example, the MONA experiment that VINCI Airports carried out at Lyon-Saint Exupéry Airport offers passengers a biometric pathway. Provided that they agree to create an account, facial recognition gates installed at the various checkpoints save them from having to present their ID documents several times. They can also receive personalised and context-sensitive commercial information. This trial combines biometric tracking and a relationship marketing solution in a single technological platform.

The few examples described above of applications involving facial, posture and behavioural recognition technologies show, through their diversity and their wide range of potential consequences, that there is no way of defining the intrinsic virtues or disadvantages of these different technologies in advance. Each use case requires a prior analysis to identify the issues, the foreseeable consequences and any potential abuses. An ethical approach needs to be reflective before it can be prescriptive.

In this case, this reflective approach is especially important, since the applications of facial, posture and behavioural recognition technologies vary from one case to the next. Some applications appear to be beneficial, while others raise problems. Some may also be both useful and harmful, depending on how they are introduced or used. It is also essential to adopt a forward-looking approach to anticipate any situations where applications that appear to be harmless today could be misused in the future.

This opinion focuses on the methodology for leading this reflective approach. It builds on the CNIL report entitled "***Facial recognition, for a debate living up to the challenges***", which was published in 2019[4][5]. This approach requires a fine-grained definition of what is meant by facial, posture and behavioural recognition, an identification of the problems that these technologies are supposed to resolve, an evaluation of the way in which they are likely to achieve those aims and the risks involved, particularly their misuse for unanticipated purposes, and lastly a rigorous experiment-based assessment into their effectiveness.

This opinion encouraged the Committee to reflect further on what approach should be taken and especially the issues at stake, which go beyond the need to protect personal data.

In addition to this introductory chapter, this opinion is divided into four chapters.

Chapter 2 clarifies and describes what is meant by facial, posture and behavioural recognition, the types of stakeholders involved in implementing these technologies, and the definitions of the associated terms.

Chapter 3 draws attention to the issues associated with deploying a system that incorporates facial, posture and behavioural recognition, and particularly the prospective methods for rigorously assessing its effectiveness. We will also discuss the epistemological aspects of this approach, which must be based on scientific experimentation. The aim is to also weigh up the potential benefits that warrant the use of these technologies against their overall economic impact. Finally and particularly from an ethical point of view, it is important to anticipate the changes in social behaviour resulting from the use of these technologies wherever possible and particularly define the necessary avoidance strategies.

Chapter 4 addresses the various tensions and ethical dilemmas.

Finally, Chapter 5 issues recommendations according to the stakeholders involved. These recommendations encompass the purpose of facial, posture and behavioural recognition systems, which should be distinguished from their usefulness, as well as the conventional notions of proportionality and transparency, the risks of bias and discrimination, the scientific and epistemological aspects of assessing these systems, the conditions of use, and finally the economic and environmental considerations.

3. France's Law of 19 May 2023 on the 2024 Olympic and Paralympic Games does not make any provisions for using facial recognition techniques or biometric identification systems. Furthermore, safeguards have been implemented to govern their use, such as giving the public prior notice, as well as an assessment of the system by members of parliament, and oversight by the CNIL

4. https://www.msdmanuals.com/fr/professional/immunologie-troubles-allergiques/d%C3% Agficits-immunitaires/syndrome-de-digeorge

5. https://www.cnil.fr/en/facial-recognition-debate-living-challenges

INSET 1

THE 2024 OLYMPIC GAMES: THE ABSENCE OF FACIAL RECOGNITION TECHNOLOGIES

In anticipation of the Olympic and Paralympic Games, which are due to be held in France from 24 July to 8 September 2024, the Law of 19 May 2023, which supplements the Law of 26 March 2018[6], allows for a number of exemptions from the applicable rules and authorises certain experiments.

The bill's impact assessment highlights the specific featuresand the scale of the Games as justification for the need to gear the law towards the specific constraints of its organisation, while respecting the principle of proportionality. Therefore, Article 10 provides that the images collected by means of a CCTV system or aircraft-mounted cameras may be subject to algorithmic processing operations for the purpose of detecting and flagging certain events, on an experimental basis. The impact assessment[7] reveals that the implementation of solutions incorporating artificial intelligence technologies is strictly regulated: The sole purpose of the processing operations is to ensure security and safety at sports, recreational and cultural events, or in public places that are particularly exposed to the threat of terrorist acts (Christmas markets, concerts, transport, etc.). Processing activities are carried out on a restricted set of images to detect predetermined events that are likely to present or reveal one of these risks, and report them so that the relevant services can intervene more effectively. In addition, algorithms only function in real time and do not work on pre-recorded images, and they exclude the use of biometric data and any biometric identification or facial recognition devices.

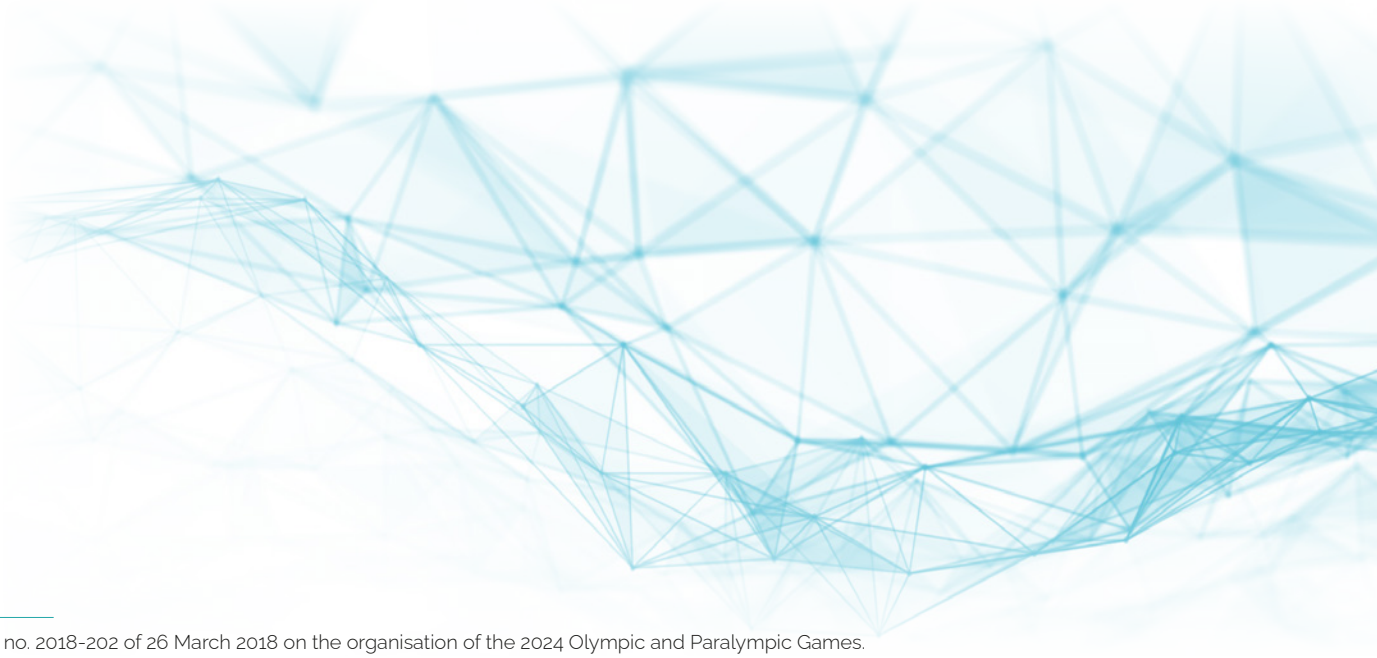
Algorithmic processing can be used to detect objects (weapons, abandoned parcels, etc.) or high-risk situations (crowd movements, people lying on the ground, and so on), but cannot be used to identify the individuals concerned.

Lastly, processing cannot be reconciled, interconnected or automatically networked with any other personal data processing operations.

This provision was met with stiff opposition, but the Constitutional Council considered that the use of algorithmic processing was supported by sufficient safeguards[8] after duly noting that there was a lack of facial recognition technologies and biometric identification systems. By endorsing the Law of 19 May 2023, the Constitutional Council ruled that these provisions did not infringe the right to freedom of movement, the right to demonstrate, the right to freedom of opinion or the right to privacy. The Council did not agree with the plaintiffs who believed that the Law violated the principle of equality (on the grounds that the criteria for algorithmic processing did not exclude any discrimination) or that it undermined human dignity by allowing (according to the plaintiffs) images to be processed by algorithms without any human intervention.

The provisions in the Law state that the algorithmic processing operations used must allow for the objectivity of the criteria and the type of data processed to be checked, as well as include human control measures and a risk management system to prevent and rectify any biases or misuse.

Finally, in terms of potentially continuing and extending the experimental system, the legislator will be responsible for drawing the conclusions from the assessment into the system and examining its effectiveness at preventing breaches of the peace while taking account of the right to privacy. In light of the foregoing, the system can be re-examined[9] for compliance with the Constitution.



6. Law no. 2018-202 of 26 March 2018 on the organisation of the 2024 Olympic and Paralympic Games.
7. https://www.legifrance.gouv.fr/contenu/Media/files/autour-de-la-loi/legislatif-et-reglementaire/etudes-d-impact-des-lois/ei_art_39_2022/ei_-spox2233026l_cm_22.12.2022.pdf.
8. Decision no. 2023-850 DC of 17 May 2023 - Law on the 2024 Olympic and Paralympic Games.
9. Note that these conclusions of the Constitutional Council are not unanimously supported by legal experts: refer to Céline Castets-Renard, "Augmented cameras: a danger for freedom during the Olympic and Paralympic Games (and beyond)?" Recueil Dalloz no. 22 2023 pp.1138-1141.

2. TECHNICAL ASPECTS AND VOCABULARY

2.1. SYSTEM COMPONENTS

2.1.1 HARDWARE COMPONENTS

First of all, a digital system offering facial, posture or behavioural recognition capabilities uses **one or more sensors,** which are designed to collect physical signals from the scene or environment where they are installed. A sensor can be a camera operating in the visible light or infrared spectrum (for collecting signals at night), a radar (for collecting signals relating to an object's position and speed of movement), a microphone or an ultrasound sensor. Several sensors can be combined, such as a camera and a microphone (to collect videos with sound). They can also be networked with communication devices to cover a wide area, like an entire city.

Sensors can be stationary, such as a camera mounted on a mast at a crossroads or in the corner of an ATM machine. There are many situations where sensors can also be mobile. For example, they can scan the environment from a fixed anchor point, such as a camera pivoting on a mast within a given angle of rotation, or they can be mounted on a mobile device, i.e. a drone or aircraft, or even on a smartphone.

A sensor can collect signals instantaneously (snapshot) or over a certain period of time, or even continuously (video).

In some cases, there are no sensors that are specifically used for recognition purposes. In other words, recognition is carried out directly by matching pre-existing digital data, such as recognising people in photos published on social media.

Finally, it should be noted that this opinion does not include devices based on sensors that are worn in contact with a person's body (e.g. for weapons detection) or which collect signals from inside the body (e.g. ultrasound sensors).

2.1.2 SOFTWARE COMPONENTS

The signals collected by the sensors are processed by software that is embedded in the actual sensors or installed in a remote device. In the second case, the signals are sent from the sensor by a specific means of communication (such as a data link). For automated recognition or recognition support applications, the software interprets the signals collected by the sensor, i.e. it transforms the raw data into meaningful information that is relevant to the purpose in question. The processing operation will result in a "yes" or "no" (a person is recognised or not), a person's name or identifier, tracking information on a person or moving object, a description of a person's behaviour ("running", "dropping off an object"), and so on.

To interpret the signals, the software requires references, which can be used to establish matches. For instance, to determine whether someone is clearly the person indicated in their passport, the software examines how closely they resemble the photo in the passport. This assessment involves calculating the similarity between various unique features in the person's image (eyes, nose, ears, etc.) and the corresponding features in the passport photo.

References can use models described by a set of characteristics. For example, in the case of behavioural descriptions, they can refer to action models comprising the action of "dropping off an object", which itself includes a sequence of sub-actions such as "moving with an object", "stopping with an object" and "moving without an object", which are associated with proximity, speed, uncertainty and other parameters1[10].

References can also be databases from which the software will calculate matches between the signals collected and the information in those databases. In its results, the software will provide the elements whose characteristics are statistically the "closest" to those in the signal collected. Machine learning algorithms can then be implemented to exploit the data and characterise a class of examples, such as an emotion.

Note that machine learning looks to acquire knowledge from past experience. Different approaches are available (reinforcement learning, group concept mapping, lazy learning, action learning, etc.). Supervised learning is the most frequently used method. It starts with a stream of labelled examples, each of which is assigned a category. It then creates a function that is capable of finding the label for each example. Note that there are many different supervised learning disciplines, such as decision trees, inductive logic programming, kernel machines and deep learning. The choice of discipline depends largely on the type of data.

10. Rim Romdhane *et al.* "Activity Recognition and Uncertain Knowledge in Video Scenes". In: IEEE International Conference on Advanced Video and Signal-Based Surveillance (AVSS). Krakow. Roland. Aug. 2013. URL: https://inria.hal.science/hal-01059602.

2.1.3 HUMAN COMPONENTS

The recognition system can be fully automated, as is the case with PARAFE[11] (automated fast-track crossing at external borders). In this particular case, professionals are available to supervise operations and intervene if necessary. However, the system can operate without any explicit human involvement, such as for recognising people in photos posted on social media. In this context, a person who has already been identified will automatically be "recognised" in other photos without anyone actually confirming or challenging the results.

The system can also be designed to provide support for professional users, for example by raising the alarm after a specific person, behaviour or situation has been identified. Operators are then responsible, with involvement from the relevant authorities if necessary, for confirming whether the information provided by the system is accurate and acting accordingly. The system comprises hardware and software elements associated with human operators. Examples of areas where such systems are used include healthcare (help in detecting pain, confirming a person's identity before surgery, etc.), security (help in detecting assaults or problematic crowd movements) and the military (help in assessing a situation).

2.2. STAKEHOLDER CATEGORIES

In the interests of accuracy, this opinion categorises the stakeholders involved in the various aspects of designing, manufacturing, implementing and using facial, posture and behavioural recognition systems. Aside from a few adaptations, the categories are based on the terminology used in the draft European regulation on artificial intelligence.

1. **Scientists**, who observe and analyse the effects of facial, posture and behavioural recognition technologies. This category also includes **designers** or **researchers** developing a signal or image processing system or method.
2. **Engineers** or **developers** working on behalf of a manufacturer and developing devices incorporating facial, posture or behavioural recognition technologies.
3. **Manufacturers** which, as their name suggests, produce and sell devices with embedded facial, posture or behavioural recognition technologies.
4. **Suppliers** or **integrators**, who design and market products or associated services. They may buy or license the product from the manufacturer to market it in their own system. They may be importers or distributors. They may also be the supplier of a service using devices that incorporate facial, posture or behavioural recognition technologies.
5. **User operators**, who acquire the system and use its results for their own operations. Examples include airport management teams, border police (PARAFE system), railway and public transport providers, shopping centres, local authorities, digital technology professionals (unlocking phones, recognising people on social media), and company management teams (access badges).
6. **Professional operators**, who are responsible for installing, supervising and maintaining the technological systems deployed. They are involved when special skills are required for implementing the system. For example, operators interpret the results provided by the system and decide what action is needed.
7. **Natural data subjects**, who are exposed to the system, whether or not they are aware of its existence and irrespective of whether they have given their consent. *Examples: passers-by, spectators at sports events, consumers, travellers, people using facial recognition on their phone, and social media users.*
8. **Legislators** (*national* or *supra-national*), who are responsible for establishing the legal and regulatory framework for deploying the technological systems. *Examples: parliament, government and European institutions.*
9. **Institutional representatives**, who are in charge of the framework for rolling out these systems. *Examples: local authorities, the Head of State, etc.*
10. **Regulators**, who are the public authorities that monitor and ensure that the recognition system is deployed in compliance with current legislation and regulations. *Examples: CNIL and ARCEP.*
11. **Certification organisations**, which carry out tests and conformity assessments with a view to authorising the deployment of a system in accordance with legislation. They may be public certification authorities or private bodies, or even actual manufacturers (self-certification), or a mandated independent body, depending on legislation.
12. **Representatives** of the various components of civil society. *Examples: trade unions, local residents' associations, consumer associations, think tanks and NGOs.*

2.3. IDENTIFYING THE NEEDS

The hardware (especially the sensors) and software used in facial, posture and behavioural recognition systems must meet an exacting requirement specification, which in turn must serve a specific purpose. The components produced must conform to the precise technical specifications set out in the requirements specification, and the manufacturer must be capable of demonstrating that its products fulfil these specifications and the stated needs.

Needs may be in response to a wide variety of motivations:

- **Efficiency**: time savings compared to manual or human action (unlocking a phone) or recognition (PARAFE)
- **Performance**: highlighting characteristics that human observers are unlikely to detect
- **Permanence**: availability over time
- **Savings**: reduction in surveillance and control staff
- **Coverage**: scale of the sensor deployment programme (in case of cameras deployed in cities)
- **Security**: detection of events that could be potentially harmful to people and property; passenger flow control (underground platforms, stadiums, etc.)
- **Policy**: implementation of public policies

11. https://www.immigration.interieur.gouv.fr/Europe-et-International/La-circulation-transfrontiere/Le-passage-rapide-aux-frontieresexterieures-PARAFE

2.4. TERMS AND DEFINITIONS

2.4.1 RECOGNITION AND FACIAL, POSTURE AND BEHAVIOURAL RECOGNITION

The term "recognition" appeared long ago in the French language and is used in many contexts with different meanings. For instance, military forces in France use the word recognise in the sense of performing reconnaissance in enemy territory to gather intel. In the legal system, it can be used in the sense of admit or acknowledge, and in some cases it can mean verification. In philosophical terms, there are at least three classic meanings of the term recognition[12]. For the first, *recognising* someone means realising that one already knows the person. In the second sense, recognise oneself is to recognise the significance of one's actions and therefore take individual responsibility for them; this is the origin of ethics. Finally, in the third sense, recognising a person[13] means attributing merit, value and respect to that person, i.e. distinguishing them from others. In the field of digital technology, recognition is partly based on the first meaning, i.e. establishing a person's identity. It is also partly due to the third meaning, since it involves categorising a person, for example classifying them according to their gender and consequently attributing a quality to them.

A distinction is made between facial recognition (face), posture recognition (body position) and behavioural recognition (movement dynamics). These three forms of recognition can be combined, such as to produce a result: "Jane Doe is running while concealing an object against her body." Vocal (voice timbre, pitch and intensity) and verbal dimensions can be added to the body dynamics to improve recognition or refine the results. In this instance, this opinion will restrict its focus to non-invasive systems, which excludes DNA analysis or brain imaging techniques. Automatic recognition modules are also distinguished by the type of signals (image, video, sound, etc.) that they accept as inputs and the sensors that collect them (cameras, microphones, and so on).

Strictly speaking, it should be noted that a digital system does not "recognise" a person in the sense defined above. It uses calculations to match signals against the data stored in its memory to find an identity or categorise behaviour. Therefore, a digital recognition system should not be likened to a human being. Only humans can truly recognise, if necessary with the help of a digital system.

2.4.2 PROCESSING OBJECTIVES: AUTHENTICATION, IDENTIFICATION AND CATEGORISATION

Irrespective of the physiological (face, voice, etc.) and behavioural features analysed and the physical signals processed, a distinction is typically made between three recognition processes[14]. In some respects, these three processes reflect the different meanings[15] of the term "recognition" as mentioned above:

Authentication aims to ensure that a person is who they claim to be. In practice, authentication is used to confirm a given person's identity based on their face. Examples include determining that the person presenting a passport is actually the person named in the passport or ensuring that the person unlocking a smartphone is the owner.
From a logical perspective, this is a "one-to-one" matching process.

Identification aims to is to identify an individual in a group of people based solely on their face, posture, gait or, more generally, their behaviour. This means that recognition systems can identify which of the individuals in the database is featured in an image or video posted on social media, or in the footage filmed by a street camera.
From a logical perspective, this is a "one-to-many" search process.

Categorisation classifies individuals according to a predetermined criterion, such as their gender, age, behaviour or emotions. Some studies even try to characterise people according to their sexual orientation16, religious or political beliefs17 or ethnic origin. Note that many of these attempts raise epistemological and ethical issues. There is no evidence that sexual, religious or political orientation is reflected in a person's physiognomic or behavioural traits.
From a logical perspective, this is a "one-to-many" classification process.

A distinction can also be drawn between **static** recognition, such as identifying an individual at a given moment in time, and **dynamic** recognition, such as tracking an individual due to the persistence of certain attributes (e.g. their clothes) in a stream of images, which does not necessarily involve identifying that individual.

12. Paul Ricoeur. *The Course of Recognition.* Ed. by Stock. Les Essais. Paris, France. Jan. 2004
13. Axel Honneth. *The Struggle for Recognition.* Passage. Paris, France: Editions du Cerf. 2000.
14. Davide Castelvecchi. "Is facial recognition too biased to be let loose?" In: *Nature* 587.7834 (Nov. 2020), pp. 347-349. doi: 10.1038/ 041586-020-03186-4. URL: https://www.nature.com/articles/d41586-020- 03186-4.
15. The definitions proposed here are different to those in ISO/IEC 2382-37:2022. https://www.iso.org/obp/ui/en/#iso:std:iso-iec:2382:-37:ed-3:v1:en
16. Despite our reservations about the quality and integrity of this work, we have included a reference for the sake of completeness (Yilun Wang and Michal Kosinski. "Deep neural networks are more accurate than humans at detecting sexual orientation from facial images", eng. In: *Journal of Personality and Social Psychology* 114.2 [Feb. 2018], pp. 246-257. doi: 10.1037/pspa0000g8)
17. With the same reservations as for the previous reference, we can cite (Michal Kosinski. "Facial recognition technology can expose political orientation from naturalistic facial images", en. In: *Scientific Reports* 11.1 [Dec. 2021], p. 100. doi: https://doi.org/10.1038/s41598-020-79310-1. URL: http://www.nature.com/articles/s41598-020-79310-1)

2.4.3 MONITORING, CONTROL AND PROTECTION

The concepts of monitoring, control and protection obviously have many different meanings, which explains why there are so many misunderstandings. In this opinion, we will use the meanings that appear to be most relevant within the field of facial, posture and behavioural recognition.

Monitoring is primarily about *keeping watch*. This is understood both in the sense of *"watching over a person for whom one has a moral responsibility"* and in the practical sense of *"ensuring that an activity runs smoothly"*[18]. But it can also mean *"closely observing and keeping informed, using policing methods, about the activities of people deemed suspicious, the behaviour of certain communities or groups, and high-risk places"*[19]. This could potentially lead to tensions between the meaning that implies protection and the meaning that implies police investigations.

Control means both *"checking something" and "voluntarily mastering one's body, feelings and instincts"*, or even *"exercising moral or political domination"*[20]. Once again, tensions could arise between simply checking that an object complies with a predefined standard and making that object subject to a standard or individuals.

Protect means to *"keep safe from harm or injury"*. The term comes from the Latin *protegere ("to cover in front of, to shelter")*, which in turn is derived from adding the prefix *pro- ("in front")* to the verb *tegere ("to cover, shelter or safeguard")*[21].

A "monitoring camera" does not actually monitor in the literal sense of the word, since it does not actually "watch" by itself, let alone gather intelligence. The camera picks up signals, and the software processes those signals. Similarly, a "video surveillance or protection system" does not protect, since it cannot keep people out of harm's way. These expressions are actually semantic shorthand for the system as a whole, which comprises sensors, software and human operators. This system can then help monitor according to one of the term's three meanings, i.e. *watching over a person, ensuring that a process is running smoothly and keeping informed through policing methods*. In this respect, note that the expression "video surveillance" in France is increasingly being replaced by "video protection", since its connotations are more reassuring (people certainly prefer to be protected than watched).

2.4.4 FUNCTION, USE AND USAGE CONDITIONS

A technology system has a clearly defined **function,** such as authentication. **Use** describes how that technology system is used, such as to check a person's identity or access a digital service. A recognition system can be installed in a public environment (e.g. the street), a private environment open to the public (e.g. an airport), an environment not open to the public (e.g. company premises) or a personal environment (e.g. for accessing a telephone or home). The **usage conditions** specify the restrictions on the system's use, such as the age limits for people passing through an automated border control system. Some of these restrictions may be influenced by regulatory requirements, including data storage periods, or even ethical issues.

18. Dictionary of the Académie Française
19. TLFi (Digitised Treasury of the French Language)
20. TLFi, *ibid.*
21. TLFi, *ibid.*

3. OPEN QUESTIONS

3.1. EPISTEMOLOGICAL ASPECTS

Above all, the **purpose** of a recognition system must always be defined in clear, precise and unambiguous terms. What exactly are we trying to achieve with this system? Detecting an assault in a car park, authenticating someone from their ID document, such as a passport, identifying a person during an interrogation or on a stretcher, analysing video tapes to track down the people appearing in the footage, determining the emotions of a passer-by or a car driver's level of fatigue, and so on. This is the first and most important point. There may be **several purposes** at the same time, some of which may be hidden. For example, facial recognition technology may be used in an airport for a number of purposes, whether increasing security, modernising the airport by offering enhanced services, improving the airport's bottom line (possibly resulting in redundancies) or speeding up operations to save time for users. These purposes reflect the interests of the various parties and stakeholders. Consequently, it is important to ensure that these different purposes are explicitly defined, bearing in mind that they serve different objectives (the desire to save time or money is not the same as the need to improve security). There is also the risk that technology devices could be misused, whether intentionally or accidentally. Therefore, the desire to tighten up security should not lead to widespread surveillance of the population or decisions that violate individual freedoms. These purposes can be debated and potentially regulated (see recommendations 5.1 and 5.6).

To meet these purposes, questions must be raised about the technological resources (hardware and software) that can be used. Steps must be taken to examine how the hardware and software will help achieve the specified purposes by **comparing the different solutions available**, without relying on an all-in-one "miracle solution" from a single supplier. The process of comparing the different technological solutions and hardware / software architectures should also be extended to encompass other existing systems (police patrols, security guards at supermarket entrances, monitors at school entrances, etc.).

Finally, the **different solutions should be analysed in terms of their effectiveness** at satisfying the initially defined purpose(s). This analysis must be based on a **rigorous and transparent experimental approach** using solid scientific foundations. For experiments to be relevant, they should mirror real-life conditions. Transparent communication of the results is essential. A simple percentage error is not enough. Explanations must be provided about what the figures actually mean, while offering background information about the experiment's conditions. Experiments should be opened up to public discussions and inquiries so that everyone can assess the consequences of introducing facial, posture and behavioural recognition systems (see recommendation 5.5).

3.2. ECONOMIC AND ENVIRONMENTAL ASPECTS

It is important to highlight the **economic aspects of deploying the various systems**, i.e. an assessment of all the expenditure required to implement those systems (see recommendation 5.7). An assessment must be carried out at a very early stage by comparing the cost of the prospective solution against the costs of other solutions, irrespective of whether or not they are based on digital technologies. The following must be taken into consideration:

- The **physical infrastructure**, meaning the sensor networks (e.g. cameras) by specifying the quantity, and their installation and maintenance costs, without forgetting their lifespan and environmental costs.
- **Processing software**, especially automatic recognition software, while remembering that data must be stored securely and software trained by learning, which entails significant economic and environmental costs.
- **The cost of setting up teams to monitor and operate the systems.** Contrary to popular belief, installing computerised surveillance systems, even if they incorporate facial, posture and behavioural recognition software, requires well-trained professional operators, which can prove expensive.
- Finally, **the costs of experimentation, validation, certification and risk assessments**.

3.3. CHANGES IN SOCIAL BEHAVIOUR

The **increasingly widespread use of monitoring and control technologies** is leading to **changes in human behaviour**, along with tacit compliance attitudes and avoidance strategies. The Chinese experience highlights these two trends. On the one hand, the entire population is subject to a stringent list of constraints, and on the other, some people are trying to escape detection through their choice of clothes, make-up and all sorts of other tricks. Therefore, the effectiveness of these technologies should be subject to an ongoing and comprehensive evaluation, not only before they are installed, but also after they have been deployed. There is every likelihood that setting up cameras in certain neighbourhoods could have the effect of shifting crime to other areas. If such monitoring and control systems are rolled out, it will be vitally important to anticipate and regularly analyse social and anthropological changes. If any aberrations are observed, such as evidence of a shift in crime, the relevant stakeholders would need to reconsider whether these systems should be deployed.

4. ETHICAL TENSIONS

4.1. TENSION BETWEEN INDIVIDUALS AND THE COLLECTIVE

Facial, posture and behavioural recognition technologies tend to create tensions between individual / collective freedoms (freedom of movement, freedom of assembly, etc.) and personal safety, which are reminiscent of the tensions between two of the meanings of the word "monitor" mentioned above: "*watch over a person for whom one has a moral responsibility*" and "*keep informed (possibly through policing methods)*". These tensions are especially hard for citizens to appreciate on account of their limited knowledge of the technologies involved and above all due to the fact that these technologies are often invisible. As a result, there is a tendency to overestimate the dangers, particularly when there are fears that their data could be over-exploited by public stakeholders, even though there are robust legal safeguards in place within the European Union[22]. At the same time, there is a tendency to under-estimate the dangers, since they are unaware of certain tracking methods, such as those used by some private companies without their knowledge, because they have failed to read the terms and conditions for the devices that they have purchased or the systems that they are using "free of charge". Whether over-estimating and under-estimating the risks, both possibilities are harmful: the first risks leading to a sense of fatalism, while the second could lead to carelessness.

The urban environment is increasingly permeated by behaviour monitoring sensors (public spaces, especially streets, public services: public transport, and private spaces: the car) operated by many different stakeholders that are rarely identified by the citizen.

The combination of systems from various stakeholders and their widespread use without an overarching vision and understanding of those systems raises the fundamental question of controlling the consequences, i.e. the prospect of cross-referencing the data collected, the potential impact of all the systems on citizens, and the effects on the individual. Ecosystems of public and private stakeholders also need to be developed for the purpose of mapping systems globally, monitoring compliance with the law and analysing any ethically undesirable effects for individuals and society. A clearer understanding of the systems and their purposes is a prerequisite for safeguarding individual freedoms; only this knowledge can lead to a consensus based on a collective debate.

To reduce the feeling of intrusion that citizens may experience when they realise that others, particularly public or private institutions (banks, insurers, ISPs, mobile phone operators, etc.), possess information about them, informed consent must be a prerequisite, barring the existence of the other legal bases provided for in the GDPR[23]. For consent to be truly informed, citizens must be able to weigh up the freedoms that they are willing to relinquish against the individual or collective benefits that they are expecting to see.

4.2. USEFULNESS VS. CONSEQUENCES

The question of **usefulness** must be asked in an objective, reasoned and well-argued manner. Basically, it cannot be estimated without exploring the benefits and drawbacks of all the potential solutions. An isolated example of using a facial, posture or behavioural recognition system in a given situation is not enough to demonstrate that those systems would also be useful in comparable situations. For instance, in the case of the Olympic Games, the scale, nature and media impact of such an event may prompt organisers and governments to use facial recognition technologies and allow economic stakeholders to roll out innovative solutions or grant them economic advantages. They may also be aiming to address a perceived sense of safety. However, it is debatable as to whether introducing a facial recognition system to open doors for athletes or staff, as was the case during the Tokyo Olympic Games in 2021, is any more useful than implementing a conventional magnetic card system.

In addition to the perceived or stated benefits of these systems, there is a need to assess the trade-off between the benefits and risks in different situations, particularly:

- Usefulness *versus* habituation: the widespread use of facial, posture or behavioural recognition systems for benefits that are not always demonstrated or reasoned can trivialise these systems and cause society to become accustomed to them, without being aware of the long-term consequences. For example, using facial recognition for payments could eventually lead to the disappearance of coins and other conventional payment instruments. Using facial recognition systems in occasional or exceptional circumstances, such as to ensure security during a major event, also raises questions on two separate levels. On the one hand, the public may lose sight of the ethical or social issues at stake, and on the other, users may benefit so much from the ease of use provided by these systems that they find it hard to cope without them in ordinary situations.
- In military and warfare applications: in the context of the war in Ukraine, for example, the initiative by US company Clearview AI (see Inset 2) to make its facial recognition solutions available free of charge to the Ukrainian people to help them fight their attackers is highly questionable from an ethical point of view. Notwithstanding the generous intentions behind this proposal (i.e. helping the Ukrainians uncover Russian infiltrators and possibly people who have committed war crimes), it should be remembered that facial recognition systems cannot identify individuals with complete certainty. The consequences of using this technology could be dramatic in the event of a mistake, and it can also spawn a number of ethical and legal risks in terms of international humanitarian law and international human rights law. It could also be anticipated that these technologies, when used for military or policing applications, will be combined with targeting actions that could be automated.

22. Note that if European citizens travelled to China, they would clearly be exposed to technologies that are prohibited in Europe.
23. The European Union's General Data Protection Regulation (Regulation (EU) 2016/679).

INSET 2

THE USE OF FACIAL RECOGNITION IN WAR CONTEXTS: MISUSE

When hostilities broke out in Ukraine, most of our fellow citizens were profoundly affected by the sight of Russia's bombing campaign and attempt to invade the country. Many people in France, in Europe and on the other side of the Atlantic wanted to do everything in their power to help the Ukrainians regain their sovereignty. Consequently, initiatives aimed at helping the Ukrainians fight back against their aggressors were encouraged. One of them caught our attention, since it involves facial recognition. US company Clearview AI offered free access to its facial recognition solutions so that the Ukrainian people could fight back against the invaders. According to an article by news agency Reuters[24], Clearview AI has considered several uses for its technologies.

The first application is to spot undercover Russian soldiers, possibly spies or saboteurs, during police checks. The idea is also to unmask people who have potentially committed war crimes during subsequent trials or unambiguously identify Ukrainian refugees.

The second application concerns Russian prisoners, by notifying their families that they have been captured, enabling families to communicate with them and then posting their photos or even videos of them in captivity on social media.

Finally, the third application relates to the bodies of Russian soldiers who have died on the front lines. Clearview AI proposes to determine their identity using facial recognition technologies and then sending their photographs to their families and friends. Due to the circumstances of the war, some people believe that Clearview AI's intentions are commendable, since they promise to give the Ukrainians a way of defending themselves.

However, it is worth pointing out that facial recognition technologies cannot identify an individual beyond all reasonable doubt, which means that there is a risk of misunderstandings with potentially disastrous results. In addition, these uses of facial recognition could have highly questionable consequences on a moral level, including injustice, humiliation, violations of the Geneva Convention on prisoners of war, and instrumentalisation and desecration of images of the dead. All such practices should be strongly condemned in any situation. Therefore, the desire to do good by helping Ukraine fight its enemy runs the risk of achieving the opposite of what was expected. More generally, even when facial, posture and behavioural recognition technologies are used for purposes that are considered to be legitimate, their effects may be questionable on ethical grounds.

- In policing applications: questions should be raised about the usefulness of implementing facial recognition systems for security purposes when the number of people checked is disproportionate to the objective (and the expected benefit) of finding a single person.
- In professional applications: there is the possibility that some types of actions or behaviour could be detected by accident. A CCTV system could perfectly detect certain actions by a company's workforce, such as romantic relationships between employees, even though this is not the intended purpose. French case law has also made reference to CCTV systems installed in stores to detect shoplifting, which actually detected thefts committed by a cashier[25]. A facial recognition system installed in a company's lift or reception area could also detect a disability in one of its customers or employees, even though the company manager is not supposed to know the person's medical file.
- In driving applications: behavioural recognition systems are gaining traction in autonomous driving applications and in advanced driver-assistance systems to detect motorists falling asleep at the wheel or to improve driving for greater safety or reduced fuel consumption. But they can just as easily inform an insurance company or manufacturer about a driver's disability, psychiatric illness or lack of attention without the user's consent or prior information.

4.3. INHERENTLY PROBLEMATIC USES

Some uses of facial, posture or behavioural recognition systems are inherently problematic. Two applications that raise ethical questions can already be identified:

- **The extraction of "sensitive" information within the meaning of the GDPR and France's Data Protection Act,** particularly the alleged detection of a person's sexual orientation, ethnic origin, political opinion and trade union membership.
- **The recognition of emotions,** especially in such situations as a recruitment process or legal proceedings.

24. Paresh Dave and Jeffrey Dastin, "Exclusive: Ukraine has started using Clearview AI's facial recognition during war", Reuters, 14 March 2022, https://www.reuters.com/technology/exclusive-ukraine-has-started-using-clearview-aisfacial-recognition-during-war-2022-03-13
25. Court of Cassation. Social Division, 20 November 1991. 88- 43.120. Published in the Bulletin, "La Pomme" judgment of 20 November 1991.

4.4. THE MATTER OF FREE AND INFORMED CONSENT

As stated in the GDPR, to be lawful, the processing of personal data must be based on consent, which constitutes a legal basis, or on some other legitimate basis provided for by the GDPR or another provision of national or EU law. However, it should be remembered that the processing of biometric data, which is considered to be sensitive data, is prohibited in accordance with the GDPR, unless the law provides for an exception based on consent and the public interest. Therefore, consent is not the only legal basis (for example, Article 9 of the GDPR allows for processing where it is necessary to protect the vital interests of the data subject, or for purposes in the public interest, or scientific research purposes), but it is important to emphasise that when data processing is based on consent, it must fulfil certain conditions. In particular, controllers should be able to demonstrate that the data subject has given free and informed consent. In its Opinion 136 on the evolution of ethical issues relating to consent in healthcare, the CCNE[26] pointed out that although consent benefits from a clear legal framework, question marks often arise about the effectiveness in obtaining informed consent. How can people consent to something that they do not understand? As with the development of new medical techniques, the significant acceleration in the use of facial, posture or behavioural recognition systems has considerably increased the complexity of the framework in which consent is required. That explains why it is important to move beyond the concept of binary consent (yes/no). Consent should be seen as a dynamic process that may evolve as part of a relationship based on mutual trust. It adapts to the individual's journey and choices, and may ultimately be withdrawn. Such refusal must be respected. For people who are unable to decide for themselves, the question arises about the capacity to decide for others.

Facial recognition systems rely on collecting biometric data, which are a special category of personal data. In accordance with the GDPR, data subjects are required to give explicit consent to the processing of their biometric data, unless another legal basis applies under the GDPR. For consent to be valid, people must be free to choose to use a facial recognition or other system without any particular constraints:

- People must be able to give free consent, which implies having a choice and being able to withdraw their consent.
- Consent must be specific and relate exclusively to the processing of biometric data. It must be obtained after information has been provided in clear and plain language.
- Consent should be unambiguous, i.e. given by a clear affirmative act by which people indicate their agreement to the processing of their personal data, such as by a written statement, including by electronic means, or an oral statement.

Although free and informed consent cannot always be obtained in practice, such as in the case of cameras installed in public spaces, or during a job interview due to the pressure that an employer might exert on a candidate, a notice must always be available to inform data subjects.

While it has not substantially changed the definition of consent, the GDPR has strengthened its content and scope to the point of making it an exception to the principle of prohibiting the processing of biometric data for the purpose of identifying a natural person (Article 9(1) of the GDPR). It is still hard to understand consent as a legal basis according to Article 9(2) of the GDPR, given the different ways in which it may be used. For example, the issues are not the same, depending on whether consent is being given for authentication or identification purposes.

4.5. HUMAN SUPERVISION

Note that facial, posture or behavioural recognition systems involve a large number of stakeholders at every stage of their existence, from design through to maintenance, as well as different parties at every level of their architecture. The many players involved and the difficulties associated with the intricate chain of interactions between humans and machines complicate the issue of liability and run the risk of diluting it. That explains why it is important to distinguish between the roles of each party and define the type of responsibility early into the process, both in legal and ethical terms. While algorithmic systems perform calculations from a mass of data to arrive at a given result, the value of that result depends on the quality of the data and the calculation and learning models, which may feature a number of biases. Therefore, the way in which the result contributes to a decision also needs to be taken into careful consideration.

It is essential to identify the ethical tensions kindled by the implementation of facial, posture or behavioural recognition technologies and the use of these systems in different contexts, with regard to the role of human beings and the "conflicts of authority" that could arise during the decision-making process. This may involve disputes about a person's identity or intentions during transit or access, the analysis of pain leading to a diagnosis or treatment, or the detection of behaviour leading to a police decision.

The consequences of a decision that affects individuals imply a responsibility that cannot be attributed to a technology, system or machine. Only human beings or organisations represented by human beings can be held legally liable for a decision affecting individuals (see recommendation 5.6),

Furthermore, algorithmic systems are subject to regulations that require such decisions to be transparent.

The prospect of sharing roles and interactions between humans and machines with the aim of improving the performance of a facial, posture or behavioural recognition system raises two tensions:

26. National Ethics Advisory Committee for Life Sciences and Health: https://www.ccne-ethique.fr/en

- The decision to implement the system is often driven by the need for quick and automated processing, meaning that real-time human supervision is ineffective; therefore, human supervision is not always a viable option.
- Humans are not infallible. They can make mistakes or be influenced by the machine's results due to automation bias.

In addition, introducing facial, posture or behavioural recognition systems in environments as diverse as transit areas, shopping centres, businesses, or medical centres, leads to question marks about training, maintenance and the human resources required to oversee the systems and make sure that they are functioning properly.

For example, this involves laying on appropriate training for system operators, so that they can understand how the systems work and examine the performance and quality of the results obtained. It is essential that operators are aware of the limitations with algorithms, particularly the presence of artifacts, the degree of precision, and the extent of any errors and failures in the system. Operators also need to be trained how to use the systems, so that they can gauge the severity of the situation and the risks involved, depending on the degree of confidence in the calculations and results produced, with the aim of best calibrating their interactions with the machine. In situations where a real-time reaction is required, this should depend on the confidence placed in the machine's results according to its performance. The design of a facial, posture or behavioural recognition system should also be aligned with the context in which the system will be used, and it should also include:

- An analysis and assessment of the reliability of the system's results (degree of detection accuracy, rate of false positives, etc.) by carrying out periodic tests.
- An interface for viewing the events detected by the system, which presents uncertainties, relevance information or explanations adapted to the need to validate results in real time.
- The possibility for the system to present several detection and interpretation scenarios, and not just the most probable one.
- Session recording capabilities (data, interpretation, human action, etc.) in anticipation of subsequent audits.

Finally, the results provided by facial, posture or behavioural recognition systems should not constitute evidence. They assist in establishing evidence through factual data collected with sensors, and they interpret those data. The results of facial, posture or behavioural recognition systems should not be considered to be absolute, but simply clues. The final decision must always be taken by the human being supervising the machine, who must be accountable, whatever the authority involved.

5. RECOMMENDATIONS

Some of the recommendations include such well-known concepts as purpose (cf. §5.1), proportionality (cf. §5.2), transparency (cf. §5.3) and fairness (cf. §5.4), which should be incorporated into the field of facial, posture or behavioural recognition technologies. Other recommendations are more specific, such as examining the scientific and epistemological aspects of the experiments (cf. §5.5) or studying the economic (cf. §5.7) and social issues (cf. §5.6) relating to the deployment of these technological systems.

These recommendations are aimed at the different stakeholders involved, which we have placed in the categories defined in Section 2.2.

5.1. PURPOSE AND USEFULNESS

The purpose refers to the desired goal, i.e. the objective that the stakeholder is consciously pursuing, which determines the intention to design, trial or market a service or use involving a facial, posture or behavioural recognition system. Tensions may arise between different purposes, since stakeholders may have diverging interests in relation to the same facial recognition system (cf. §2.3) and may pursue potentially different objectives (e.g. airport managers will aim to streamline passenger flows, security services will focus on safety, and customers will tend to emphasise the speed and efficiency of the system). Usefulness is the real, tangible or even auditable benefit for the service's target audience. Purpose and usefulness should not be confused. However, comparing one to the other can help determine the rationale for using facial, posture or behavioural recognition technologies or, conversely, limiting or prohibiting their use. Therefore, the **purpose** must be specified in plain and unambiguous terms, while demonstrating the system's **usefulness** in relation to that purpose. Usefulness must be examined by several parties on an experimental basis and with tangible results. Consequently, this opinion issues the following recommendations:

RECOMMENDATION 5.1.1

(USER-OPERATORS, LEGISLATORS)

Clarify the purpose(s) of using a facial, posture or behavioural recognition system in a given context, while clearly demonstrating its usefulness in relation to the purpose(s). Emphasise the reasons for using the system in a particular place or situation.

RECOMMENDATION 5.1.2

(USER-OPERATORS, LEGISLATORS)

Produce a risk map of the rights and freedoms of the people affected by the use of a facial, posture or behavioural recognition system. Compare the risks against the reason for using the system.

RECOMMENDATION 5.1.3

(USER-OPERATORS, LEGISLATORS)

To identify and prevent abuses in relation to the purpose(s) of the facial, posture or behavioural recognition system, plan and describe the procedures for regular inspections and consultation with the various external auditors and certification bodies, while emphasising their independence. It is also important to take account of feedback.

INSET 3

INCREASINGLY WIDESPREAD USE OF FACIAL RECOGNITION SYSTEMS IN EUROPEAN AIRPORTS: TREADING A LINE BETWEEN CAUTION AND TRIVIALISATION

On 26 October 2023, Frankfurt Airport announced that it was bringing its facial recognition system into widespread use, making it the first airport in Europe to provide all passengers with the option of passing through security checkpoints using biometric technology exclusively from check-in to boarding. In Germany, other airports such as Hamburg and Munich offer this technology, but only to a limited extent, since it is only available to certain passengers (Lufthansa or Star Alliance). In addition to these initiatives, the International Air Transport Association (IATA) is looking to promote the use of biometric identification technologies in airports by highlighting the results of its surveys, which tend to show that passengers are in favour of processing their biometric data if it speeds up the various procedures. In France, Lyon Airport has been experimenting with facial recognition technology since 2020, and Paris-Orly Airport is also preparing to trial the technology for boarding passengers. However, the prospect of a fully digital and secure air transport system based on biometric identification (using a "digital travel credential"[27] if applicable), such as promoted by IATA[28], has not met with unanimous approval in Europe and is likely to divide the national regulatory authorities on their interpretation of the GDPR, especially when it comes to the storage of certain categories of personal data.

27. https://www.businesstravel.fr/Laeroport-de-franc- fort-generalise-la-reconnaissance-faciale.html
28. https://www.air-journal.fr/202i-n-i6-iata-ce-que- veulent-Les-passagers-du-transport-aerien-5231669. html

In France, for example, the data protection authority (CNIL) expressed its reservations about the conditions for storing administrative and technical data[29] that are collected and stored locally for the purpose of carrying out statistical analyses on the performance of facial recognition algorithms, in its deliberation no. 2016-012 of 28 January 2016, following a referral from the Minister of the Interior[30].

The CNIL also drew attention to the "significant risks" that facial recognition technologies pose to individual freedoms in an environment "characterised by a growing number of CCTV systems, which could theoretically allow for the mass roll-out of facial recognition systems, with increased risks for data protection and privacy."

Finally, the French authority stressed that "this technology's performance, which has yet to be implemented by the State on a large scale, remains to be demonstrated." The lingering doubts voiced by some stakeholders, despite surveys showing that travellers have a certain amount of confidence in biometric technology, and the caution surrounding the widespread use of facial recognition technologies in Europe, point to a tremendously varying landscape: the deployment of facial recognition systems continues to be significantly localised, and trials are still ad hoc and highly regulated, despite pressure from associations of air transport companies that are broadly in favour of seeing biometric technologies mainstreamed in airports.

This lack of harmonisation raises questions in a Europe that is keen to promote free competition and the free movement of people, while ensuring a high level of protection for fundamental rights and safeguarding competitiveness in its market. A different system in each airport could prove to be harmful to both businesses and individuals, who expect to be treated in the same way, since the GDPR is intended to apply in all EU Member States.

5.2. PROPORTIONALITY

Proportionality is an essential concept, since it helps strike a fair balance between the means and the end and, where necessary, establish a balance between different purposes. In particular, proportionality involves fulfilling certain conditions, such as the appropriateness of an action (the planned action should be capable of effectively achieving the aim pursued, which has been defined in tangible terms) and its necessity (the action is necessary in relation to what is required to achieve that aim). In the case of a technological system, proportionality is understood in terms of the purposes for which it has been designed and deployed. Proportionality is assessed according to various criteria, which may be incommensurable, such as the impact on rights and freedoms, the environment, society and democracy, as well as the economic cost and effort.

Note that proportionality in relation to the purposes of a technological system should not be confused with a risk-benefit analysis.

RECOMMENDATION 5.2.1

(SCIENTISTS, LEGISLATORS, INSTITUTIONAL REPRESENTATIVES, USER-OPERATORS)

Using tangible arguments (based on real evidence), assess the proportionality, i.e. the necessary and appropriate nature, of the use of facial, posture or behavioural recognition technologies in relation to the purposes defined in a tangible and objectively verifiable manner through studies carried out at different times and in each context. Also take account of any unintended consequences, particularly processing of any information that has been collected by mistake.

5.3. TRANSPARENCY

Transparency is a multi-faceted concept. One of these facets involves informing people. For example, employees should be informed if facial recognition systems are used in the workplace, such as by means of cameras.

Another aspect is the overall methodology, which should be explained so that all stakeholders can take an informed position, especially before the event. Finally, transparency relates to the preliminary studies that must be described in detail and whose conclusions, whatever they are, must be widely disseminated.

RECOMMENDATION 5.3.1

(MANUFACTURERS, INTEGRATORS)

Provide operators, regulators, institutional representatives and user-operators with a description of the system's hardware and software architecture, the data acquisition and processing methodology used, the tests performed and the learning base.

RECOMMENDATION 5.3.2

(USER-OPERATORS, SCIENTISTS)

Explicitly state the purposes for which facial, posture or behavioural recognition systems are used, so that no purposes are overlooked or concealed. Conduct reliability and impact assessments into the facial, posture or behavioural recognition systems based on accurately defined experiments carried out rigorously at every stage of the project, and then publicise the assessment findings through transparent but responsible disclosures (to protect the security of the information systems).

RECOMMENDATION 5.3.3

(ALL INTERESTED PARTIES, ESPECIALLY LEGISLATORS AND THE MEDIA)

Use appropriate terms when talking about facial, posture or behavioural recognition systems and avoid approximations that could be misleading and create false representations, whether in specifications, official texts or the media.

29. This includes data collected after scanning the passport, the characteristics of the passport, its holder, the travel dates and destinations, the quality of the passport photo and the photo taken when checking in, the match between both photos and the authenticity of the passport data.

30. https://www.Legifrance.gouv.fr/iorf/id/JORF- TEXT000032372514

5.4. BIAS AND UNJUSTIFIED DISCRIMINATION

Facial, posture and behavioural recognition systems may include biases (cf. Inset 5), leading to unjustified discrimination (cf. Inset 6) or misinterpretations.

Biases must be prevented to anticipate the risks of discrimination that are likely to occur. This involves examining the distribution in training data, analysing any potential sources of bias, and finally carrying out tests. It is important to repeat these studies at regular intervals to avoid any discrepancies. In this respect, it is worth pointing out the large corpus of scientific studies that have recently focused on these issues[31].

INSET 4

PLAIN LANGUAGE

The quality of discussions on the use of these technologies requires a certain level of semantic rigour, including when it comes to summarising or popularising texts that need adapting or simplifying due to their technical content. Wherever practicable, certain formulas should either be forbidden or accurately defined. By way of example, the following is a list of expressions that have been associated with the use of facial, posture or behavioural recognition technologies:

- "Smart CCTV" or "smart video surveillance" instead of facial, posture or behavioural recognition systems or, more generally, algorithmic image processing systems.
- "Smart", "augmented" or "algorithmic cameras" for cameras combined with facial, posture or behavioural recognition software programmed using artificial intelligence techniques. In other words, the sensor should not be confused with the technologies used to process the information collected by these sensors.
- "Artificial intelligence" or "AI" instead of systems programmed using artificial intelligence techniques.
- *"The incredible pretention that Article 7 of the law has of entrusting a non-human authority with managing millions of images captured in the public space is an unprecedented attack on the fundamental rights to security and dignity."*[32] The term "non-human authority" is nonsense, because there are people and institutions behind any computer system that must remain accountable for the consequences of their acts.

"If the algorithm considers that certain characteristics, such as the decision to wear a particular garment or the colour of a person's skin, are more likely to be associated with the risk that needs to be identified, (...) it means that the use of an algorithmic CCTV system is a potentially discriminatory and racist practice"[33]; note that algorithms are not people; they "do not consider" in the proper sense of the term.

INSET 5

BIASES

According to the traditional sense of the word and in the context of this opinion, a bias is a deformation or a flaw; more specifically in the technical sense, it is *"1. a distortion, a systematic deformation of a statistical sample chosen by a defective procedure, or of an evaluation or 2. the difference between the mathematical expectation of an estimator and the quantity to be estimated."*[34] This should also include the fact that some biases stem from subjective considerations, such as the conscious or unconscious tendency to favour or disadvantage certain categories of people based on their name, hobbies or other criteria.

Although in the literature on algorithmic fairness, bias is often synonymous with discrimination, it should be remembered that not all biases will necessarily lead to discrimination and that not all discrimination is the consequence of bias. Discrimination obeys a precise legal definition, so that only biases resulting in unjustified differences in treatment between individuals should be considered to be discriminatory (see Inset 6).

Since algorithms are designed by human beings, any biases likely to lead to discrimination may reflect prejudices that are already present in society. If these biases are not identified, they run the risk of leading to systematic discrimination. Biases can creep into databases and also into all the stages involved in specifying, developing, deploying and maintaining these systems.

INSET 6

DISCRIMINATION

Discrimination, according to sense A (without the idea of unequal treatment) in the Digitised Treasury of the French Language[35], is the act of differentiating, with a view to separate treatment, between elements by identifying them as distinct. In sense B (with the idea of unequal treatment), discrimination is understood to be the differential treatment applied to people based on unjustified criteria.

According to French and European law, discrimination is any practice, even seemingly neutral, that is likely to put people at a particular disadvantage compared to others, unless that practice is objectively justified by a legitimate aim, and the means to achieve that aim are necessary and appropriate. Discrimination includes any actions associated with one of the following grounds: actual or assumed membership or non-membership of an ethnic group or race, sex, religion, beliefs, age, disability or sexual orientation. Discrimination on any of these grounds is prohibited in relation to social protection, healthcare, social benefits, education, access to goods and services, or supply of goods and services[36].

31. Luciano Floridi. The ethics of artificial intelligence: principles, challenges and opportunities - Mimesis Philosophie, 2023
32. *Appeal to the Constitutional Council on the bill relating to the 2024 Olympic and Paralympic Games and various other provisions,* submitted by Mrs Mathilde Panot on 17 April 2023. p. 13
33. *ibid.* p. 12
34. https://www.larousse.fr/dictionnaires/francais/biais/9021
35. http://atilf.atilf.fr/dendien/scripts/tlfiv5/visuel.exe?26; s=1905154725;r=2;nat=;sol=0;
36. Law no. 2008-496 of 27 May 2008 containing various provisions for adapting to EU law in the field of anti-discrimination.

RECOMMENDATION 5.4.1

(USER-OPERATORS, SCIENTISTS, DEVELOPERS AND OPERATORS)

Due to the potential presence of biases, the results of the facial, posture or behavioural recognition system must be used with caution and discernment. When these systems are installed, there must be explicit mention of the potential presence of biases, especially for operators.

RECOMMENDATION 5.4.2

(SCIENTISTS)

Promote research into evaluating facial, posture or behavioural recognition systems for the purpose of qualifying, assessing and limiting any biases wherever possible.

5.5. SCIENTIFIC AND EPISTEMOLOGICAL ASPECTS

Whenever there are plans to roll out a facial, posture or behavioural recognition system, it is important to implement a rigorous scientific approach based on objective observation data to ensure that the experimental protocols and systems implemented demonstrate that the planned technologies are fit for purpose.

The first phase involves clearly identifying the **objectives pursued** in each case, such as protecting legitimate interests - public safety, public health, public order, protection of people and property, etc. Subsequently, assumptions must be made about the way in which the proposed technological systems contribute to achieving the objectives and their added value compared to existing systems. Finally, **experiments** are required to scientifically confirm or disprove the assumptions. For this reason alone, such experiments are legitimate. For an experiment to be justified, its purposes must be clearly stated and the protocol well defined (see Inset 7).

INSET 7

SCIENTIFIC AND LEGAL EXPERIMENTATION

On a scientific level, an experiment involves making a variety of repeated observations by modifying certain initial conditions in a controlled manner. Conditions may relate to the value of certain parameters, or the presence or absence of a given factor, such as a device. This allows scientists to establish a link between the parameters, the factor and the observations. Provided that changes to the parameters are well distributed, an experiment can therefore confirm or disprove assumptions about the characteristics of the observations.

Experimental approaches can also be found in public action, where they have pronounced legal implications. Within the field of public policy, authorities with legislative or regulatory powers, including independent administrative authorities and local / regional authorities[37], may carry out "experiments", subject to complying with a certain legal framework[38]. These experiments cover a variety of realities, since they may be performed within an existing legal framework or they may require a new rule offering exemption from applicable law. The Conseil d'État has also pointed out that legal experimentation for assessing how a reform should be implemented is a particularly appropriate tool for measures designed to "test new digital systems" (such as artificial intelligence and facial recognition software for the police) "when they need to be developed sequentially, in direct contact with their users, and are subject to regular evaluation"[39].

Like scientific experiments, legal experiments must satisfy certain methodological requirements. The Conseil d'État has listed the essential principles as follows: an accurate definition of the assumptions and objectives, a specified deadline for obtaining convincing results, the possible constitution of a sample, the collection of data for comparison purposes, and the prior determination of the success criteria and assessment proceduresd[40]. Although France's growing use of the experimental method in public policy design reflects a certain degree of progress in both policy development and evaluation methods, the Conseil d'État has advised that the departments responsible for designing and conducting these experiments often have "insufficient knowledge of this methodology"[41]. This shortcoming is detrimental, because it can distort public debate. Another pitfall has been noted. In other words, the competent authorities sometimes set up an experimental scheme, not to ensure that a reform is relevant, but to facilitate its uptake "since the use of experiments has a reassuring effect". Lastly, as pointed out by the Conseil d'État, some reforms may be adopted due to the growing number of experiments requested from private stakeholders. Therefore, experimentation in the legal sense of the word is somewhat complex, since it needs to avoid two pitfalls, namely political instrumentalisation (e.g. in the context of an unpopular reform) and excessive epistemological rigour. In the last case, the Conseil d'État stated that while the methods of the experimental sciences can, in some cases, be replicated for public policy experimentation, raising "scientific rigour to the same level as a legal requirement that applies to any public policy experimentation would discourage the use of this method in a large number of cases where it could prove valuable and where it could be productive at a lower cost."

37. Therefore, the Constitution authorises the legislator to empower local authorities to provide exemptions, on an experimental basis, from applicable legislation and regulations.
38. Insofar as the experimental provisions of a law or regulation create a waiver from the principle of equality, they are strictly regulated.
39. Study by the Conseil d'État. "Experimentation: how to innovate when conducting public policies", adopted on 4 July 2019. French documentation.
40. *Ibid.*
41. For an example of "fake experiments" that are not accompanied by a minimum level of methodology and an experimental protocol, cf. CE. AG. 3 April 2014, no. 388486.

Consequently, this opinion issues the following recommendations:

RECOMMENDATION 5.5.1

(ALL STAKEHOLDERS)

Consistently define a protocol that specifies the purposes (scientific, usage, testing of a new business model, etc.), the assumptions, the details for implementation (equipment and method), the parties involved, the framework (place and circumstances) and the duration, for any experimentation with a facial, posture or behavioural recognition system.

RECOMMENDATION 5.5.2

(INSTITUTIONAL REPRESENTATIVES)

Consistently set up an independent audit to validate and monitor the protocol, which should be subject to regular reports. These reports must be made available to stakeholders upon request. In addition, objectively assess the conditions for obtaining the success rates claimed by certain facial recognition systems.

RECOMMENDATION 5.5.3

(SCIENTISTS, USER-OPERATORS, LEGISLATORS)

Do not describe the operational deployment of a facial, posture or behavioural recognition system as experimental unless it is part of a clearly defined and justified scientific or legal context.

RECOMMENDATION 5.5.4

(SCIENTISTS)

Encourage interdisciplinary research, that combines social sciences, law, computer science and engineering, into the design of experimentation protocols for facial, posture or behavioural recognition systems, into the interpretation of their results, and into the evaluation, verification, validation and certification procedures.

In France, several experiments involving facial recognition have been carried in publicly accessible areas in recent years. Notable examples are the trials carried out by the City of Nice (during the carnival in February-March 2019) and Aéroports de Paris (these trials were delayed due to the health crisis and ultimately took place between March and July 2021 and between February and April 2022). The CNIL did not object, since the experiments respected the principles of the GDPR. However, none of these experiments led to the systems actually being installed on a permanent basis. It should also be noted that in a Senate report published on 12 May 2022, the rapporteurs recommend prioritising experimentation within the framework of a law where facial recognition technology is concerned. Adopting an experimental law would help determine the relevant uses of biometric recognition. According to the senators, the experiment could be authorised for a period of three years, which would require the government and parliament to reassess the need and redefine the framework depending on the results obtained. The report recommends a public and independent assessment to examine how effective the technology would be in the specified use case. This assessment would be conducted by a committee of scientists and specialists in ethical issues, whose reports would be made public[2]. More recently, the Law of 19 May 2023 relating to the 2024 Olympic Games authorised (on an experimental basis until 31 March 2025) the processing of images collected by fixed cameras or mounted on aircraft at venues hosting sports events.

INSET 8

EXPERIMENTATION AND "REGULATORY SANDBOXES": STIMULATING

The OECD AI Principles of 2019 state that governments should consider using "experimentation to provide a controlled environment in which AI systems can be tested and scaled up." As such, public authorities would be able to promote an agile policy environment that supports transitioning from the research and development stage to the deployment stage for trustworthy AI systems[42]. Experimentation allows regulators to test new economic, institutional and technological approaches, and legal provisions outside of prevailing regulatory structures. Experimental regulatory approaches include innovation hubs, regulatory sandboxes, standardisation and co-regulation involving regulators and markets[43]. In its 2023 report on "regulatory sandboxes", the OECD states that these are promising for areas with fast innovation cycles, such as artificial intelligence. Sandboxes that bring together regulators and businesses enable the authorities to work with companies in testing innovative products and services without being constrained by the existing legal framework. Companies obtain a waiver from specific certain legal provisions or compliance processes to allow them to innovate, while benefitting from tailored legal support for a specific project (based on trial-and-error). Sandboxes are subject to certain conditions, since they are temporary, with a testing process usually limited to six months. Finally, it should be emphasised that the technical and market information and data collected help the authorities assess whether specific legal frameworks are fit-for-purpose or need to be adapted.

42. OECD. Recommendation of the Council on Artificial Intelligence. OECD/LEGAL/0449
43. Regulatory sandboxes in artificial intelligence. OECD digital economy papers July 2023 No. 356

INSET 9

RECOGNITION RATE

The success rates claimed for certain facial recognition systems should be treated with a degree of caution. In fact, the meaning behind certain figures is often absent or obscure. The stated "recognition percentage" should be accompanied by a description of the conditions in which the system was used and a definition of the evaluation methodology. In addition, it is known that the performance of facial recognition, whether human or automated, depends on the lighting quality, the resolution of the sensors and images, the frame, and so on.

5.6. USAGE CONDITIONS

When implementing any kind of technological system, particularly systems using facial, posture and behavioural recognition or, more generally, biometric data, it is important to determine the conditions justifying its use. The following recommendations are intended to clarify the questions that should be asked about the social and political context in which the system will be deployed.

RECOMMENDATION 5.6.1

(OPERATORS, USER-OPERATORS)

Ensure that the conditions for using the facial, posture or behavioural recognition system are always strictly in line with its declared purpose. Inform data subjects so that they can carry out a check and be encouraged, where appropriate, to request that checks be carried out.

RECOMMENDATION 5.6.2

(REPRESENTATIVES OF SOCIETY, USER-OPERATORS, OPERATORS)

Carry out regular assessments, through independent certification bodies, into the effective use of facial, posture or behavioural recognition systems and be capable of drawing on the conclusions of these assessments.

RECOMMENDATION 5.6.3

(USER-OPERATORS, OPERATORS)

Keep a close eye on the place that human operators occupy within facial, posture or behavioural recognition systems, the skills that they are required to have, the roles that they need to retain, and the risks that could be caused by both their presence and absence. Such systems should be considered as part of a general review of the social organisation within which they are embedded.

RECOMMENDATION 5.6.4

(OPERATORS, USER-OPERATORS, DATA SUBJECTS, REPRESENTATIVES OF SOCIETY)

Conventional methods, without using biometric data, must remain accessible to both operators, such as in the event of a fault, and data subjects if they so desire. This should be the case in airports and for payments, where the use of alternative methods must be allowed that are not penalising for users, especially in terms of process times.

5.7. ECONOMIC AND ENVIRONMENTAL ASPECTS

Systems incorporating facial, posture or behavioural recognition technologies are expensive to develop, maintain and implement. Many believe that they would have the effect of downsizing the number of jobs in surveillance. However, humans are essential for monitoring the alerts issued by these systems. Therefore, it would appear to be necessary to weigh up the cost of these systems against other means that would be capable of achieving the same objectives just as effectively. Besides, there is more than just a financial cost involved. The process of deploying the cameras and training / running the algorithms has a significant environmental impact.

Consequently, this opinion issues the following recommendations:

RECOMMENDATION 5.7.1

(USER-OPERATORS, LEGISLATORS)

Evaluate all the resources required to implement systems that include facial, posture or behavioural recognition technology. These resources include the initial expenditure on hardware and software infrastructures, as well as the costs incurred by staffing requirements and maintaining the installations.

RECOMMENDATION 5.7.2

(USER-OPERATORS, SCIENTISTS)

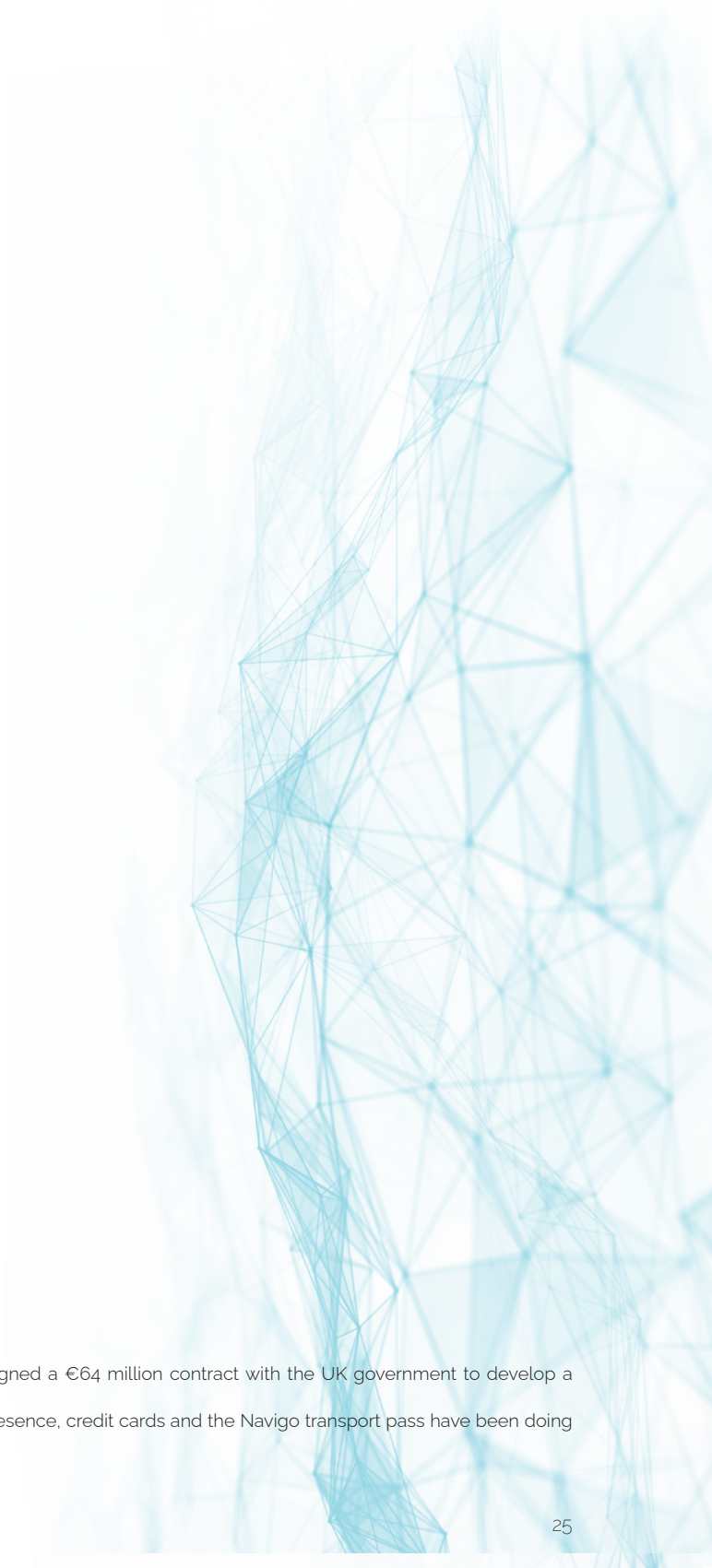
Compare the financial and environmental costs of facial, posture or behavioural recognition systems against those of all other solutions, so that a reasoned choice can be made based on ethical, financial and operational considerations. Carry out studies into the impact on jobs, skills, working conditions, social relations and the environment.

6. CONCLUSION

We would like to stress the legitimate concerns that many people have expressed about facial, posture or behavioural recognition technologies, especially when they are used in public spaces, where they could infringe individual and collective freedoms. These fears have led to proposed regulations and even moratoria on a national, European and international level from state or supra-state institutions, such as the European Parliament and the European Commission, as well as from certain industrial groups. In its resolution of 20 January 2021 on artificial intelligence, the European Parliament "invites the Commission to assess the consequences of a moratorium on the use of facial recognition systems". Similarly, in the European Commission's proposal for a regulation dated 21 April 2021, Article 5 proposes prohibiting, barring certain exceptional situations, "the use of real-time remote biometric identification systems in publicly accessible spaces for the purpose of law enforcement", which includes facial, posture and behavioural recognition technologies. Note that IBM announced in June 2020 that it was withdrawing from the facial recognition sector due to concerns about its use for mass surveillance and racial profiling. However, IBM's subsequent actions quickly seem to contradict this ethical stance1[44].

All this proposing, hesitating and procrastinating reveal the unease currently surrounding the widespread use of these technologies. At the same time, there are applications that may prove to be beneficial to both communities and individuals alike, including the protection of individuals in response to authentication needs, the justice system to help carry out investigations, culture (which is experimenting with oculometry or eye tracking in museums), and the health sector. Therefore, proposed regulations should weigh up the usefulness, benefits and risks of the various applications. This attempt to strike the right balance raises problems when looking to introduce a general ban or moratorium on research into facial, posture or behavioural recognition technologies, especially since such research is not specific and is used in other areas (object recognition, scene recognition, etc.).
All applications for facial, posture and behavioural recognition technologies should consequently be examined with the greatest of care, discernment and caution, including their effects, bearing in mind that in this field as in many others, simplistic arguments, whatever their source, are both harmful and counter-productive. An approach must be adopted that is transparent and supported by rigorous experimental assessments into these technologies' performance. The results must be contrasted against the needs that these technologies are designed to meet. Finally, it is vitally important to keep a close eye on how these technologies are used over time in an effort to avoid harmful misuses.

The widespread use of so-called surveillance technologies, of which facial, posture or behavioural recognition is a component, has an impact on relationships between people, lifestyles and therefore the human condition. These changes are occurring little by little and insidiously "without anyone actually realising that they are happening". In this context, and even though social control is anything but a new issue[45], it is important to raise citizens' awareness of these developments so that they are capable of democratically deciding on the society in which they wish to live, by arbitrating between the need for security, the benefits of the conveniences provided by these technologies, and the risks to individual and collective freedoms.



44. After publicly distancing itself from facial recognition in 2020, IBM signed a €64 million contract with the UK government to develop a national biometric platform.
45. Concerns about "what people will say" and questions about police presence, credit cards and the Navigo transport pass have been doing the rounds for a long time.

7. ACKNOWLEDGEMENTS, HEARINGS AND WORKING GROUP INVOLVED

7.1. ACKNOWLEDGEMENTS

We would especially like to thank the following people whom we interviewed or who helped us in preparing this opinion.

We obviously assume full responsibility for any errors or inaccuracies.

7.2. PEOPLE INTERVIEWED

- **Véronique Borré**
  Deputy Director General of Security for the City of Nice
- **Sébastien Louradour & Lofred Madzou**
  World Economic Forum
- **Maryne Cotty-Eslous**
  CEO and Founder of Lucine
- **Xavier Fischer**
  CEO of Datakalab
- **Emmanuel Bloch**
  Director of Strategic Information at Thalès
- **William Eldin**
  Co-Founder of XXII
- **Olivier de Mazières, Elisabeth Sellos-Cartel and Michel Cadic**
  Ministry of the Interior and Overseas France
- **Gaëtan Goldberg**
  Technology & Human Rights Adviser at the Defender of Rights in France
- **Claire Nicodeme**
  SNCF
- **Xavier Chapuis and Fabrice Sabourin**
  RATP
- **Félix Tréguer and Arthur Messaud**
  La Quadrature du Net
- **Romain Galesne-Fontaine and Yann Haguet**
  IN Group
- **Tanguy Bertolus**
  CEO of Lyon Airport
- **Pascal Débordé**
  Project Manager in the IT Division at Aéroports de Lyon
- **Natacha Liaboeuf**
  Lawyer at Aéroports de Lyon

7.3. COMPOSITION OF THE WORKING GROUP

- **Raja Chatila**
- **Laure Coulombel**
- **Laurence Devillers**
- **Karine Dognin-Sauze -** co-rapporteur
- **Jean-Gabriel Ganascia -** co-rapporteur
- **Claude Kirchner**
- **Catherine Tessier**
- **Célia Zolynski**

accompanied by:

- **Mélanie Gornet** (intern)
- **Anaëlle Martin** (writer)
- **Alexia Pronesti** (writer)
- **Amélie Turci** (writer/intern)

8. BIBLIOGRAPHY

Castelvecchi, Davide.
"Is facial recognition too biased to be let loose?"
In: *Nature* 587.7834 (Nov. 2020), pp. 347-349.
doi: 10.1038 / 041586 - 020 - 03186 - 4.
URL: https://www. nature.com/articles/d41586-020-03186-4.

Castets-Renard, Céline.
"Augmented cameras: a danger for freedom during the Olympic and Paralympic Games (and beyond)?"
In: *Recueil Dalloz22* (2023), pp. 1138-1141.

Science and Technology Ethics Commission.
"The ethical issues raised by facial recognition"
In: *8th Youth Commission* (2020), p. 46.

Ethics Board of the Allistene Digital Sciences and Technologies Alliance.
Research Ethics in Machine Learning.
Tech. rep. CERNA, 2017.
http://cerna-ethics-allistene.org/digitalAssets/53/53991_cerna ___thique_apprentissage.pdf.
CNIL (French data protection authority).

Facial recognition, for a debate living up to the challenges.
Tech. rep. 2019.
URL: https://www.cnil.fr/sites/cnil/files/atoms/files/facial-recognition.pdf.

Defender of Rights.
Biometric technologies: the obligation to respect fundamental rights.
Tech. rep. 2021.

EDRi and EIJI.
"A legal analysis of biometric mass surveillance practices in Germany, the Netherlands, and Poland".
In: *The rise and rise of biometric mass surveillance in the EU* (2021), p. 160.

Floridi, Luciano.
The ethics of artificial intelligence: principles, challenges and opportunities.
Passage. Paris, France: Mimesis Philosophie, 2023.

Honneth, Axel.
The Struggle for Recognition.
Passage. Paris, France: Editions du Cerf, 2000.

Kosinski, Michal.
"Facial recognition technology can expose political orientation from naturalistic facial images".
In: *Scientific Reports* 11.1 (Dec. 2021), p. 100.
doi: https://doi. org/10.1038 / S41598 - 020 - 79310 -1.
URL: http://www.nature.com/ articles/s41598-020-79310-1.

Martinez-Martin, Nicole.
"What are Important Ethical Implications of Using Facial Recognition Technology in Health Care?"
In: *AMA Journal of Ethics* 21.2 (Feb. 201g), E180-187.
ISSN: 2376-6980.
doi: 10.1001/amajethics.2019.180.
URL: https://journalofethics.ama-assn.org/article/what-are-important-ethical-implications-using-facial-recognition-technology-health-care/2010-02

Moosavi- Dezfooli, Seyed- Mohsen *et al.*
"Universal Adversarial Perturbations".
In: *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition* (CVPR). July 2017.
VOIE project (open and integrated video protection)

Ricœur, Paul.
The Course of Recognition.
Ed. by Stock. Les Essais. Paris, France, Jan. 2004.

Romdhane, Rim *et al.*
"Activity Recognition and Uncertain Knowledge in Video Scenes".
In: *IEEE International Conference on Advanced Video and Signal-Based Surveillance* (AVSS).
Krakow, Poland, Aug. 2013.
URL: https://hal.inria.fr/hal-0i05c1602.
Secur ED. en-US. May 2020.
URL: https://www.secur-ed.eu/ (visited on 01/07/2022).

The Lancet Digital Health.
"On the face of it"
In: *The Lancet Digital Health* 3.10 (Oct. 2021), e612.
ISSN: 25897500.
doi: 10.1016/S2589- 7500(21) 00217- X.
URL: https://linkinghub.elsevier.com/retrieve/pii/S258975002100217X (visited on 10/01/2021).

Wang, Yilun and Michal Kosinski.
"Deep neural networks are more accurate than humans at detecting sexual orientation from facial images"
In: *Journal of Personality and Social Psychology* 114.2 (Feb. 2018), pp. 246-257.
doi: 10.1037/pspa0000098.

ALPHABETICAL INDEX

9. APPENDICES

9.1. OPEN CONSULTATION OF THE CNPEN

9.1.1 PURPOSE OF THE DOCUMENT

The CNPEN was set up in 2019 under the authority of the National Ethics Advisory Committee for Health and Life Sciences (CCNE). It examined the ethical issues raised by the use of automatic recognition technologies (facial, posture and behavioural recognition).

This open consultation is aimed at gaining a clearer insight into people's perceptions of automatic recognition technologies based on their own everyday experiences. The idea is to foster a constructive debate about the ethical issues raised by these technologies and promote a technology that serves the common good. The responses to this open consultation are intended to enhance the Committee's discussions and refine its perception of the ethical issues inherent in recognition technologies.

This consultation is divided into two parts:

- The first part addresses various questions relating to your perception and experience of facial recognition technologies. This part mainly comprises closed questions that sometimes lead to more open-ended conditional questions. It also includes a few open-ended questions that are generally optional. This part will take between 15 and 30 minutes to complete.
- The second part is optional. Questions cover more technical issues (errors in automatic recognition systems, data retention, etc.) and require more detailed answers. This part will take approximately 10 to 15 minutes to complete.

USE AND PROTECTION OF YOUR PERSONAL DATA

We do not require your first name or surname. Only IP addresses will be kept for a given period of time. The personal data requested (sex, gender, age and occupation) or which you may provide spontaneously in your responses to the consultation will only be processed if they are useful for the Committee's analysis and review. All the data collected will be stored on LimeSurvey's server in Germany and will be processed while maintaining strict confidentiality by CNPEN personnel or members of the CNPEN working group on facial recognition. Data will be stored for no more than 18 months after the consultation has ended and up to 12 months after the Committee has published its opinion.

According to the conditions defined by France's Data Protection Act of 6 January 1978 and the European General Data Protection Regulation, which became effective on 25 May 2018, all contributors have the right of access, the right to rectification, the right to query, the right to restriction of processing, the right to data portability and the right to erasure for all their personal data. Each contributor may also object to the processing of their personal data on legitimate grounds.

Contributors may exercise all the foregoing rights by contacting the CNPEN at the following address: consultation-reconnaissance@ccne.fr.

Online consultation

The consultation has been uploaded to the LimeSurvey platform and can be accessed via this URL: https://survey.ccne.fr/96563. There were 239 contributions to this consultation.

9.1.2 INTRODUCTION

What are facial, posture and/or behavioural recognition systems?

Facial recognition involves identifying, authenticating or categorising a person based on their facial features using an algorithm and reference data. Posture recognition involves analysing a person's gait and body position. Behavioural recognition refers to the process of identifying people's behaviour, such as by taking an analytical look at the dynamics of their movements. These technologies work alongside machine learning, which is a branch of artificial intelligence that uses big data. The different types of use will be covered during this consultation.

WHAT ARE THE DIFFERENT TYPES OF RECOGNITION?

There are several types of recognition - authentication, identification and categorisation - which are implemented according to the required application.

- Authentication is used to ensure that a person is who they claim to be. In practice, authentication is used to confirm a given person's identity based on their face. Examples include determining that the person presenting a passport is actually the person named in the passport or ensuring that the person unlocking a smartphone is the owner. From a logical perspective, this corresponds to a "one-to-one" matching process.
- Identification aims to identify an individual in a group of people based solely on their face or gait, which is known as a one-to-many search. This means that recognition systems can identify which of the individuals in the database is featured in an image or video posted by one of your friends on Facebook, or in the footage filmed by a street camera.
- Finally, categorisation classifies individuals according to a predetermined criterion, such as their gender, age, behaviour or emotions. Some studies even try to characterise people according to their sexual orientation, religious beliefs, political opinions or ethnic origin. From a logical perspective, this is known as one-to-many comparison. Note that these attempts raise epistemological and ethical issues. There is no evidence that sexual, religious or political orientation is reflected in a person's physiognomic or behavioural traits.

9.1.3 FOREWORD

You are responding to this consultation:

- ☐ As a representative of a group
- ☐ As an individual

Age group:

- ☐ Under 25
- ☐ Between 25 and 45
- ☐ Between 45 and 65
- ☐ Over 65

Gender:

- ☐ Male
- ☐ Female
- ☐ Other

Your location:

- ☐ Large city
- ☐ Medium-sized city
- ☐ Small town
- ☐ Country village

Educational background:

- ☐ Science
- ☐ Law
- ☐ Economics
- ☐ Literature
- ☐ Humanities and social science
- ☐ Medicine
- ☐ Other (give details)

Occupational category:

- ☐ Student
- ☐ Retired
- ☐ Actively employed
- ☐ Unemployed
- ☐ Other

FIRST PART OF THE CONSULTATION:

9.1.4 THE ETHICAL ISSUES OF AUTHENTICATION USING AUTOMATIC RECOGNITION

1. Use a recognition system to authenticate your identity for private purposes

a) Have you ever used a facial recognition system to authenticate your identity?

- ☐ Yes
- ☐ No
- ☐ Don't know

If so, under what circumstances?
Multiple-choice questionnaire with comments

- ☐ Unlocking a digital device (smartphone, tablet, computer, etc.))
- ☐ Apps (banking, social security, etc.)
- ☐ Other

b) If you had the choice between unlocking your digital device (smartphone, tablet, computer, etc.) with facial recognition, fingerprint recognition or a password, which would you choose? Why? (You can choose more than one answer)
Multiple-choice questionnaire with comments

- ☐ Facial recognition
- ☐ Fingerprint recognition
- ☐ Password

c) In your opinion, what are the advantages and disadvantages of using an authentication system based on facial recognition?
d) Has your relationship with unlocking devices through fingerprint recognition changed since the feature first appeared? If so, why?

- ☐ Yes
- ☐ No
- ☐ It depends

2. Be authenticated by a recognition system Authentication is increasingly used in the public sphere. For example, the PARAFE facial recognition software has been introduced in French airports to authenticate passengers; in the United States and China, these systems are used in schools.

a) Have you ever been authenticated using automatic recognition?

- ☐ Yes
- ☐ No
- ☐ Don't know

If so, under what circumstances?
Facial recognition technologies could be used to authenticate pupils and students at school and college entrances. A number of French colleges have decided to trial the system to detect potential intruders. This technology would be used alongside existing badge-based access control systems: Students would need to present their badge or a picture on their phone, which would be scanned, and a camera would compare the student's face against the image recorded in the college's database.

b) At the present time, this type of check is carried out using badges or visually by a person. If a facial recognition system were introduced, what do you think the additional benefits would be? What about the drawbacks?

9.1.5 THE ETHICAL ISSUES OF IDENTIFICATION

1. Identification using facial recognition in our digital applications (entertainment apps, etc.).

Our smartphones and social media use identification techniques for recognising and tagging people in photos.

a) Have you ever been asked to use facial recognition to identify people in the photo album on your smartphone or on one of your social media sites (Facebook, Instagram, etc.)?

- ☐ Yes
- ☐ No

If so, do you use this feature?

- ☐ Yes
- ☐ No
- ☐ It depends

Do you like it?

- ☐ Yes
- ☐ No
- ☐ It depends

Has your opinion changed since this feature first appeared on social media? If so, in what sense? Why?

- ☐ Yes
- ☐ No
- ☐ It depends

b) On social media, people sometimes create an account using another person's photo without their consent (e.g. a well-known public figure). To offer their users greater protection against identity theft, some social media analyse users' profile photos using facial recognition identification systems. When an individual's face is recognised in a photo associated with someone else's profile, an alert is sent to the person concerned.

What do you think about these facial recognition identification technologies on social media in terms of security and freedoms?

2. Security through facial recognition

Facial recognition identification is an increasingly popular topic in public debate. Facial recognition can be carried out retrospectively or live (i.e. in real time). Live facial recognition is currently prohibited in France, except in specific cases, such as experiments. In France, the authorities in Nice carried out a controlled live recognition trial during the 135th Carnival in 2019 with the aim of demonstrating the system's security potential.

a) Do you know if you have ever been analysed by a live facial recognition identification system?

- ☐ Yes
- ☐ No
- ☐ Don't know

b) In your opinion, is the use of this technology justified on security grounds?

- ☐ Yes
- ☐ No
- ☐ It depends

If you answered "yes" or "it depends":

Experiments involving live facial recognition are currently authorised (refer to the experiment by the authorities in Nice). However, the European Commission recently proposed that its use in public places should be prohibited except in highly specific cases.

In which cases do you think that a ban / authorisation is justified?
If not, why?

Post-processing:

Facial recognition software does not necessarily work in real time, but uses video recordings. By way of an example, this type of system can help find a suspect or missing person by analysing CCTV footage[1]

c) Which of the following uses for this type of system do you think are justified? Why?
(You can choose more than one answer)

- ☐ Find a suspect as part of a police investigation
- ☐ Find a missing person (child, person suffering from an illness, etc.)
- ☐ Recognise people who have taken part in an illegal or banned demonstration
- ☐ Other (give details)

d) Which of the following uses for this type of system do you think are unjustified? Why?
(You can choose more than one answer)

- ☐ Find a suspect as part of a police investigation
- ☐ Find a missing person (child, person suffering from an illness, etc.)
- ☐ Recognise people who have taken part in an illegal or banned demonstration
- ☐ Other (give details)

e) Should the use of facial recognition in public places be explicitly mentioned? Give details.
Multiple-choice questionnaire with comments

- ☐ Yes
- ☐ No
- ☐ It depends

f) In your opinion, a growing number of automatic recognition experiments: (give your answers - you can choose more than one answer)
Multiple-choice questionnaire with comments

- ☐ Would be needed to improve these technologies. Would lead to these technologies entering widespread use.
- ☐ Would help people get used to these technologies.
- ☐ Don't know.

1. https://www.assemblee-nationale.fr/dyn/opendata/AVISANR5L15B3404-tVII.html_Toc256000026

3. Identification technologies for flow management applications: tracking people whose identity is known

Flow management involves providing access to a service by tracking people using facial recognition. These systems are starting to gain traction in airports, such as Tokyo, where your face is used as your passport and boarding pass. In some countries, payments using facial recognition technologies have been introduced in supermarkets.

You are in a supermarket that uses facial recognition for payments. You can choose the facial recognition checkout or the traditional payment checkout.

a) There is no queue at either checkout. Which checkout do you choose? Explain your choice.

- ☐ The checkout without facial recognition
- ☐ The checkout with facial recognition
- ☐ Either one

b) There is a long queue at the traditional checkout. Which one do you choose? Explain your choice.

- ☐ The checkout without facial recognition
- ☐ The checkout with facial recognition
- ☐ Either one

c) Do you think that it is necessary to maintain a traditional system that does not use facial recognition?
Multiple-choice questionnaire with comments

- ☐ Yes
- ☐ No
- ☐ It depends

d) Do you agree with the use of this type of system? Give details.

- ☐ Yes
- ☐ No

4. Identification technologies in flow management applications: tracking people whose identity is unknown

Facial recognition technologies are sometimes used to track people without actually knowing their identity. In supermarkets, public places and public transport, these systems can also be used to improve flow management.

a) Do you have any experience with this type of system?

- ☐ Yes
- ☐ No
- ☐ Don't know

If so, under what circumstances?

b) Do you agree with the use of this type of system? *With comments*

- ☐ Yes
- ☐ No
- ☐ It depends

9.1.6 THE ETHICAL ISSUES OF CATEGORISATION

1. Categorising in the commercial and professional sphere

In the labour market, US companies use various apps to conduct video interviews. The app detects non-verbal cues, such as facial expressions, eye movements, body movements, details of the clothing worn and voice nuances. These data are then processed by the algorithm, which assigns a score to the candidate based on the employer's expectations.

a) Do you agree with the use of such an app? Why?

With comments

- ☐ Yes
- ☐ No
- ☐ It depends

In the field of marketing, categorisation can be used to profile users with the aim of offering them personalised services.

b) Do you like receiving these types of personalised ads?

- ☐ Yes
- ☐ No
- ☐ It depends

Fictional case: you want to subscribe to an online streaming service to watch films and TV shows. The service offers two different subscription plans: one with automatic facial recognition that detects your emotions to send you targeted ads, and the other without facial recognition.

c) You can choose the first subscription plan and pay half the price, or the second plan and pay the full price. Which one do you choose? Why?
Multiple-choice questionnaire with comments

- ☐ The plan with facial recognition
- ☐ The plan without facial recognition

2. Categorising to maintain public order

In the field of public order, automatic recognition could be used to detect aggressive behaviour, apprehend suspects and also detect littering or dog fouling.

a) Do you think that the use of behavioural recognition technologies is justified for detecting specific types of behaviour in underground stations, car parks, crowds, etc.?
With comments

- ☐ Yes
- ☐ No
- ☐ It depends

b) Behavioural recognition can also be used to detect aggressive behaviour at mass public events that are exposed to the risk of terrorism (Olympic Games, etc.). What do you think about this application in terms of security and freedoms?

3. Categorising in education.

a) In the Chinese city of Hangzhou, all pupils' behaviour is monitored for the purpose of "improving educational standards". Cameras have been fitted in classrooms to monitor the schoolchildren's reactions and concentration levels, as well as their emotions. An alert is sent to the teacher if they misbehave or lose concentration.

●As a parent, would you agree to your children being subjected to facial recognition at school?

With comments

- ☐ Yes
- ☐ No
- ☐ Don't know

●As a student, would you agree to this type of system?
With comments

- ☐ Yes
- ☐ No
- ☐ Don't know

●As a teacher, would you agree to this type of system?
With comments

- ☐ Yes
- ☐ No
- ☐ Don't know

b) What are the advantages and disadvantages of using behavioural recognition systems in education?

c) In the case of invigilating remote exams, the computer's camera could track the student's eye movement to prevent cheating.

How do you see remote exam invigilation using behavioural recognition in terms of the value of the exams and freedoms? Explain your answer.

4. Categorising in the healthcare sector

Categorisation can also be used in the healthcare sector, such as to detect signs of an infection during a health crisis. In some areas (airports, businesses, etc.), thermal imaging cameras combined with a facial recognition system have been used to identify signs of an infection with the Covid-19 virus and check that people are wearing a mask:

a) Do you think that the use of this type of technology to detect people's temperature is justified? To detect if they are wearing a mask? Why?
With comments

- ☐ Yes for checking people's health and that they are wearing a mask
- ☐ Yes for checking people's health, but not whether they are wearing a mask
- ☐ Yes for checking whether people are wearing a mask, but not their health
- ☐ No for both
- ☐ Don't know

b) Some systems use facial, voice and posture recognition to identify, measure and analyse the user's pain.

Under what circumstances would you agree to the use of this type of system for detecting pain? Why?
With comments

- ☐ For people who are able to express themselves
- ☐ For people who are unable to express themselves
- ☐ Other

5. Categorising according to supposed ethnic origin, political opinions, religious beliefs, trade union membership, sexual orientation, etc.

Some researchers have suggested that facial recognition technologies could be used to determine not only personality traits, but also certain orientations (political, sexual, religious, etc.).

a) Do you think that it is acceptable and justifiable, insofar as technologies are capable of doing so, to use recognition technologies to detect a person's ethnic origin, political opinions, philosophical and religious beliefs, trade union membership or sexual orientation? Why?

- ☐ Yes
- ☐ No
- ☐ It depends

b) How would you react if an association or political party used this type of technology to recruit its members?

In the case of the GendNotes note-taking app used by the police in France, some characteristics may be collected if they are considered to be strictly necessary, including supposed sexual orientation, religious beliefs, political opinions and ethnic origin. Some associations fear that automatic recognition technologies will be added to this app.

c) Do you think that there is any justification for using automatic recognition technologies to build up an accurate profile of a wanted person for security purposes?
With comments

- ☐ Yes
- ☐ No
- ☐ It depends

6. Categorising during public events

How do you see the use of facial recognition technologies during public events?
Give details.
With comments

- ☐ For security purposes
- ☐ For statistical purposes

9.1.7 CONCLUSION: CONFIDENCE AND AUTOMATIC RECOGNITION TECHNOLOGIES

Digital recognition technologies are currently one of the hottest topics in public debate, and they are beginning to create a major divide, especially in terms of the trust that people place in them.

1. In your opinion, which technology(ies) (authentication, identification and/or categorisation) raise(s) the most important ethical issues? Why? (You can choose more than one answer)
With comments

- ☐ Authentication
- ☐ Identification
- ☐ Categorisation

2. Does the type of operator have an influence on your level of trust in facial recognition technologies - in particular, do you have more / fewer / just as many / no fears about your data being processed by government operators than by private companies' operators (e.g. GAFAM[2] or BATX[3]?
Justify your choice.

- ●To detect if people are wearing a mask in the street:

- ☐ More fears about data processing by government operators
- ☐ More fears about data processing by private companies' operators
- ☐ Just as many fears in both cases
- ☐ No fears

- ●To identify people in the street in real time (searching for suspects, identifying routes, etc.):

- ☐ More fears about data processing by government operators
- ☐ More fears about data processing by private companies' operators
- ☐ Just as many fears in both cases
- ☐ No fears

●To identify people in recorded images (videos / photos):

- ☐ More fears about data processing by government operators
- ☐ More fears about data processing by private companies' operators
- ☐ Just as many fears in both cases
- ☐ No fears

- For signing into an app:

- ☐ More fears about data processing by government operators
- ☐ More fears about data processing by private companies' operators
- ☐ Just as many fears in both cases
- ☐ No fears

3. Would your answer be different if we were talking about other digital technologies? Explain your answer.

4. Users: Are you aware of human operators supervising automatic recognition applications? Do you think that this is sufficient? Explain your answer.

- ☐ Yes, I am aware that these applications are supervised by human operators and I think that this is sufficient
- ☐ Yes, I am aware that these applications are supervised by human operators, but I do not think that this is sufficient
- ☐ No, I am not aware that these applications are supervised by human operators

5. Operators: Are your applications supervised by human operators? Is this sufficient? Explain your answer.

- ☐ Yes, our applications are supervised by human operators and I think that this is sufficient
- ☐ Yes, our applications are supervised by human operators but I do not think that this is sufficient
- ☐ No, our applications are not supervised by human operators but I think that they are necessary
- ☐ No, our applications are not supervised by human operators and I do not think that they are necessary

6. What democratic bodies or arrangements would you trust for controlling the development of these new facial recognition technologies?

Thank you for completing our consultation. The following part is optional, so you can stop here or continue if you wish. It addresses the cross-cutting ethical issues relating to recognition technologies, especially the matter of mistakes by recognition systems and personal data storage. The questions may be more technical and sometimes require a longer answer than the previous section.
Would you like to continue?

- ☐ Yes
- ☐ No

*If so, please continue with the second part of the consultation. *Otherwise, this is the end of the consultation.

2. Google, Apple, Facebook, Amazon and Microsoft
3. Baidu, Alibaba, Tencent and Xiaomi

SECOND PART OF THE CONSULTATION

9.1.8 CROSS-CUTTING ETHICAL ISSUES RELATING TO AUTOMATIC RECOGNITION TECHNOLOGIES

1. Errors and recognition systems

Facial recognition algorithms can be unreliable. They may result in statistical biases, just like human beings[4], who can make cognitive mistakes. For example, to distinguish between a wolf and a dog, the recognition system starts with what it has been taught[5], namely that there are more wolves than dogs in the snow. Therefore, a dog on a white background could be incorrectly identified as a wolf. A similar phenomenon can occur with facial recognition technologies, especially when the learning database is not representative of the entire population on which they will be used.

a) Users and consumers: have you ever experienced an authentication error by a facial recognition system?

- ☐ Yes
- ☐ No

For users: if so, what were the circumstances?

For operators: what are the most common errors?

For users and operators: what do you think the consequences could be if the algorithm fails to authenticate a person? If these errors repeatedly affect certain people?

b) In the case of an identification system that could allow law enforcement agencies to apprehend wanted persons, what are the consequences if the algorithm makes a mistake?

c) Now consider the case of categorising job candidates with a recognition system. What could the consequences be if the algorithm makes a mistake?

d) Operators: what measures are you taking or could you take to limit these consequences?

Algorithms[6] have been designed to create a unique and imperceptible perturbation for each type of facial recognition system. This perturbation causes images to be misclassified with high probability. For example, instead of recognising a microwave or fridge, the image recognition system will classify it as a pillow, whereas the human eye will not see any change.

e) Operators: what do you / should you watch out for to prevent this type of problem?

2. Data use and retention

Recognition systems use the personal data of the users or people whom they are designed to authenticate. According to the GDPR, personal data retention is limited in time, and this period of time is decided by the controller in line with its specified objectives and to the extent permitted by the applicable legal framework. In the case of smartphones, data processing is not subject to the GDPR, provided that a number of conditions are met. In the case of a company, however, the data will need to comply with the GDPR and be stored for a specific period of time.

a) Operators: when deploying these technologies, do you keep users' data? If so, how?

b) Users: in which applications of digital recognition systems would the use and storage of your personal data pose a problem for you? Why?

c) Users: does the type of operator (government, company, etc.) influence your reticence or confidence in the use and storage of your personal data?

With comments

- ☐ Yes
- ☐ No
- ☐ It depends

If you answered "yes" or "it depends", which one(s) do you trust the most and why?

d) Does the location or context for storing your data also influence your reticence or confidence?

- ☐ Yes
- ☐ No
- ☐ It depends

If you answered "yes" or "it depends", which are you most reticent about and why?

e) Operators: does the origin of the software influence your decision to deploy?

f) Operators and users: in your opinion, are appropriate measures in place for using and storing the data? Do you think that the types of measures are sufficient? Explain your answer. *With comments*

- ☐ Yes, the measures taken are appropriate and sufficient.
- ☐ Yes, the measures taken are appropriate, but not sufficient.
- ☐ No, the measures taken are neither appropriate nor sufficient.
- ☐ Don't know

3. Governance of facial, posture and behavioural recognition technologies

When it comes to the ethical issues raised by authentication, identification and categorisation using facial, posture and behavioural recognition technologies:

Do you agree that these technologies should be freely used or do you think that their use should be controlled? Justify your answer.

Multiple-choice questionnaire with comments

- ☐ Everyone should be able to use these technologies, whether for personal use or for deploying in public spaces.
- ☐ A supervisory authority is needed to monitor and regulate the data (e.g. entrust this duty to the data protection authority, a citizens' association, etc.).
- ☐ A certification scheme should be implemented for these technologies.
- ☐ These technologies must be restricted to highly specific applications.
- ☐ These technologies must be completely banned, whatever the area of application.
- ☐ A moratorium is required on the use of facial, behavioural and posture recognition technologies in public spaces. Specify how this moratorium could be used.
- ☐ A moratorium is required on experiments involving facial, behavioural and posture recognition technologies in public spaces and publicly accessible areas. Specify how this moratorium could be used.

4. In this case, it is an image, and the mistakes made by human beings are not of the same type.
5. In this introduction, the term "learning" or the "system learns" is used, which is an anthropomorphism, but it seems easier for explaining the idea here.
6. Seyed-Mohsen Moosavi-Dezfooli *et al.* "Universal Adversarial Perturbations". In: Proceedings of the IEEE *Conference on Computer Vision and Pattern Recognition (CVPR)*. July 2017.

9.2. SUMMARY OF THE CONTRIBUTIONS TO THE CONSULTATION

9.2.1 GENERAL SENSE OF THE CONTRIBUTIONS

Firstly, we noted that most respondents do not use or do not wish to use facial recognition technologies. Respondents mention the intrusive nature of these systems and the potential security or totalitarian abuses that may occur. Other arguments relate to the systems' technical limitations, such as the lack of reliability, security flaws, malfunctions, and the risk of errors in the results.

Among respondents who use or are more inclined to use these types of technological artifacts, the main criteria are practicality, usability and speed. There is a degree of tension about getting used to these technologies, with some people seeing them as a risk while others consider them to be part of the natural order of things. For example, some contributors highlight the fact that the use of automatic recognition technologies for statistical purposes would lead to the widespread use of these systems. Secondly, we have observed a change in opinions according to the case studies:

- One-off and short-term deployments seem to be more acceptable and legitimate.
- Some uses seem more justified than others, e.g. tracking people in an airport in comparison to a shop. This is associated with the purpose. The first case involves border crossing security, while the other is about increasing speed at the checkout.
- The safeguards implemented have an influence on people's acceptance of these systems. An effective and comparable alternative, data anonymisation, guaranteed effectiveness of the system, and the importance of consent are just some of the factors that need to be taken into account.

Other deployments appear to be unacceptable. Examples include the use of automatic recognition technologies to detect a person's ethnic origin, political opinions, philosophical and religious beliefs, trade union membership and sexual orientation. Thirdly, the contributors reveal a number of tensions:

- **Between freedom and security:** for example, when it comes to authentication at school entrances, parents explain that they would be more reassured if such systems were implemented, but it would also hinder children's freedom and emancipation. The issues of autonomy and integrity also reflect this tension. Some respondents believe that facial recognition technologies can be used when the security of a city or the country is at stake, while others see it as "democratic heresy". These systems must be accompanied by response teams, otherwise they serve no purpose. The case of demonstrations clearly highlights the tensions between security and freedom: security for demonstrators and citizens, and the freedom to demonstrate.
- **Concerning free and informed consent:** respondents reveal the fact that consent cannot always be requested. Opinions differ about the need for a notice to inform data subjects. Respondents consider that minors cannot provide free and informed consent, especially when the system is rolled out at a school or university (e.g. behavioural recognition during remote exams).
- **Concerning the type of operator**: this can influence acceptance among users. Most respondents have just as many fears, regardless of whether the state or a private company is involved, but the trend tends to show greater apprehension towards private companies. This is justified by the fact that companies market the data. However, a few contributors mentioned reservations about the recognition systems deployed by the government. These fears are attributed to the government's binding powers. Several contributors have confidence in the government as something that "should be done".

Several contributors question whether the technologies deployed are proportionate to their purpose. In a number of cases, the use of automatic recognition technologies is not considered to be proportionate to the purpose. This aspect is reflected in the responses on the use of behavioural recognition systems for invigilating remote exams. Many contributors emphasised that the system was useless and suggested that the assessment procedures should be reviewed instead. It is also important to avoid the belief that technology is the solution for everything.

Opinions highlight the anthropological changes caused by these technological solutions. Several people are concerned that social relationships are being dehumanised (recruitment, student/teacher relations, etc.). Contributors stress the impact of these technologies when minors are the target. These concern the child's healthy development, autonomy, creativity and sociability.

Many respondents feel that the use of these technologies gives the impression of living in a society where risks are constant, which raises question marks about the level of "real" danger, the escalation in security, and keeping the population in a state of fear.

The technical limitations of these technological systems are a recurring theme in the opinions, which challenge their use. Some practices are considered unacceptable by a majority of respondents, including categorisation based on supposed ethnic origin, political opinions, religious beliefs, trade union membership or sexual orientation. One opinion described this technology as deeply racist.

Finally, contributors highlight the need to supervise and contextualise these technologies, and implement effective safeguards and alternatives.

- **The processing operations that raise the most ethical issues** Respondents highlight the link between the different uses (authentication, identification and categorisation) and consequently the fact that all of them elicit ethical issues, even though identification and categorisation seem to raise more. As far as identification is concerned, opinions differentiate between identification with and without consent, as well as explicit consent or consent without the user's knowledge, considering that the use of identification technologies is acceptable when consent is given, whereas their use is tantamount to surveillance if consent has not been obtained. Categorisation is seen as dangerous and discriminatory with too many abuses. One contributor emphasises that individuals are more complex than any imaginable category; two other contributors refer to categorisation as the only process that "really poses a problem".

- **Human supervision**

Certain respondents were not aware of human operators supervising these systems, even though some stressed the need for such human supervision. Most of those who are aware that human supervision is used do not find such measures to be sufficient, and some mention that purely informative mechanisms fall short as well. Generally speaking, opinions mention the need for human supervision, while stressing that efforts must continue to be made in this area. One opinion asks the following question: "The real issue is whether the supervisor is smarter than the machine?" As for operators, half consider that human supervision is necessary or have at least implemented such measures, while the other half have not set up such arrangements and do not consider them necessary. One contributor implies that human supervisors would also need to be supervised in this case.

- **The democratic bodies or arrangements that people trust to control and develop new technologies**

Contributors mention elected bodies, independent authorities, the data protection authority (several contributions stressed the need to reinforce its powers), specific associations, the Defender of Rights, the French National Agency for Information Systems Security, NGOs, ethics committees, public debates, the State, the CNPEN and the Constitutional Council, with compulsory training and a citizens' council with specialists.

- **Second part of the questionnaire**

In terms of the errors that contributors found in the results produced by recognition technologies, particularly in the case of authentication using facial recognition, they occur when unlocking personal electronic devices (smartphones, computers, etc.). As for search errors, they happen when people from the same family are involved, or when a user's appearance changes, such as for unlocking a banking app or with the PARAFE border control system. The most common errors are non-detection and cognitive biases.

The consequences that contributors mentioned when faced with repeated authentication errors are sometimes immediate (loss of mobility, denied access to rights, unfounded accusations, wasted time, etc.) and occasionally long term (the impact on other people's confidence in the individual, discrimination, stigmatisation, legal errors, social exclusion, and rejection towards the use of technologies). In the case of using identification technologies for apprehending wanted persons, the potential consequences mentioned include arresting the wrong person (i.e. the "real culprit" is still on the loose), a waste of police time, and the physical and psychological impacts on the individual in question. As for categorisation technologies used for recruitment purposes, this can lead to challenges about the candidates' suitability and qualities (psychological consequences), dehumanised relationships, discrimination, recruitment problems for the company, and the loss of a job for the candidate. This wastes time and has an economic cost.

To limit these consequences, operators recommend banning such systems, consistently keeping "humans in the loop", and building models that can readily be explained. Some operators advise that when a perturbation is noticed, they report it, so that tests can be carried out to determine what is causing the problem. They explain that occasional checks are required to ensure that no changes have been made by a third party and that the algorithm is still effective.

One respondent explains that storing user data on cloud servers presents fewer risks than storing them locally, while another explains that data are stored in an unusable cache memory. One respondent argues that there is no way to comply with the GDPR all the time, while others consider that data should only be retained if necessary as part of the regulation, or not at all. They can also be stored on the smartphone without being sent back to operators/manufacturers. Users believe that the purpose has an influence on the extent to which they will agree to let their data be stored, and some consider that their data should never be retained. Half of the respondents claim that the operator has an important influence on their confidence or reluctance to let their data be used and stored, and their comments reflect their ambivalent relationship with the State. The other half believe that the operator has no influence and that it is mainly the type of data that matters. Most contributors also take the location into consideration, and they have more confidence in European countries that are subject to the GDPR and which demand greater transparency. In this context, insufficient measures are taken to prevent abuses, and some consider that they are not appropriate.

Most respondents state that not everyone should have the power to use these technologies for private or public use. Opinions about the supervisory and regulatory authorities tend to be divided, with some considering them necessary, while others do not. They also have mixed feelings about restricting technologies to certain applications, since they believe that the explosion in these technologies would prevent any attempts to limit them. Most respondents felt that there is no need to introduce a certification scheme, that these technologies should not be banned and that there should not be a moratorium on technologies or trials, especially since experiments can help improve these technologies.

9.2.2 CONTRIBUTORS REQUESTING CLARIFICATION OF CERTAIN ASPECTS (VOCABULARY, CHOICES, THE COMMITTEE'S STANDPOINT, ETC.)

- **Clarification of the subject covered by the opinion**
  - On the rights in the GDPR. One opinion mentions the fact that individuals whose data are collected should have the right to withdraw their data. However, there are rights in the GDPR to achieve this, such as the right to erasure, the right to dereference content, and the right to freeze data.
  - Alternative solutions. Opinions show that people are sometimes unaware of the alternatives to facial recognition that are available to them. For example, facial recognition does not have to be used on a smartphone. A password and fingerprint can be used instead.
  - Technical aspects

The first point relates to how systems are ineffective at recognising people when wearing a mask. This comment is frequently made, even though today's automatic recognition algorithms have been tweaked to account for this situation, meaning that this is no longer a limitation for the technology.

The second point concerns fingerprints. In the following comment, the contributor considers that fingerprints do not constitute a means of authentication: "Fingerprints provide identification information, not authentication information

(like the face), since they are deemed to be public (we leave them everywhere). This is always the same fundamental error. I would advise you to refer to the basic concepts of cryptography again (unless such confusion is intentional and not simply a matter of ignorance)."

A third point that emerged in the contributions concerns the type of system used: are they adaptive or automatic systems? "Firstly, because the term "automatic" does not accurately convey current developments in artificial intelligence. It would be better to talk about adaptive systems. Secondly, because technology is evolving so fast that there is no way today to predict what tomorrow's identification systems will be.

Finally, there may clearly be risks to our privacy, but this has always been the case with human societies looking to control themselves, and it is better to follow technology and understand its potential uses instead of burying our heads in the sand. A tool is designed to provide a function, but it cannot predict all the different ways in which it may be used. A knife is used for cutting, such as cutting an apple, but it can also be used to kill your neighbour." »

A contributor corrects a question that is considered to have been wrongly asked: What do you think about these facial recognition identification technologies on social media in terms of security and freedoms? "I would correct this question as follows: Social media use facial recognition for a multitude of purposes. The primary use is probably not to detect cases of identity theft, since that does not generate any money for the platform. However, reproducing a person's social graph more effectively (even for people who are not registered) on that platform is probably the real motivation that has prompted the Internet giants to create this technology."

One opinion questioned the use of recognition technologies to assess pain by highlighting the fact that pain is experienced in various ways by different people. Resistance to pain depends on a number of parameters. This contribution highlights the opportunity presented by this type of system, i.e. they can give a sense of importance to the pain felt by the patient. It refers to the Pediatrics journal, which presented a study on facial recognition-based pain measurement software (FACS) in 2015, and to Dr Chantal Delafosse.

Finally, one opinion questioned the use of the expression "who are able to express themselves". "(...) Multimodal bodily expression is possible in the vast majority of cases, meaning that the question is one-sided, just like the obvious answer: the biometric recognition system is superfluous in this case." »

- **Request for clarification about the Committee's standpoint**

On several occasions, the comments address the Committee with the pronoun "you" to ask whether or claim that this consultation legitimises the use of this type of technology. Sometimes, the wording leads to confusion. Here are a few examples: "You're using convenience to force consent! It's always no!" "Are you trying to legitimise the use of facial recognition technologies through completely trivial examples?" "The way in which the question has been worded seems to be misleading, since it's likely to prompt a response that approves of adopting facial recognition", "And it's serious, because your answers suggest that you're trying to impose it, regardless of what respondents think!" "No. The tool is disproportionate to its effectiveness. Just take a look at the reports on CCTV systems... Cost versus effectiveness. Your proposal is indecent!"

- **Concerning the vocabulary used**

Several contributors questioned the vocabulary used. The use of the term "security" can be troubling and confusing, since it is not the systems that provide security, but the police officers or security agents using the automatic recognition systems.

Many contributors raise questions about the use of the term "individual", its definition and what it covers. The term "suspect" is also questioned, and the contributor clarifies that "suspect" does not mean guilty.

One opinion highlights the confusion between "technology" in the usual sense of the word and artificial intelligence algorithms: "Talking about "technology" shifts the problem onto the tool instead of focusing on a design that incorporates actual human choices. Even with fairly simple tools, a distinction must be made between a kitchen knife, a hunting knife or a bayonet, for example. The intention behind their manufacture is clearly not the same."

9.2.3 EXAMPLES OF THE CRITICAL CONSIDERATIONS RAISED BY PARTICIPANTS

ETHICAL DEBT

One contributor highlights the "ethical debt" created by the economically motivated widespread use of recognition technologies.

LACK OF FLEXIBILITY IN THE TECHNOLOGY

For example, authentication at schools can deny access to someone arriving in an emergency.

ACCULTURATION OF YOUNGER PEOPLE

Some contributors highlight the fact that exposing children to new technologies can have the effect of automating social control, social regulation, the loss of data, and attacks on public and individual freedoms,

PASSIVE VS ACTIVE CONSENT

One contributor points out that fingerprints require a voluntary action, whereas facial recognition technologies can be used without the individual's knowledge.

INCREASE IN INEQUALITY, BIAS AND DISCRIMINATION

Many contributors highlight the increase in inequality that such systems can cause due to algorithmic biases and also their aims. For example, in case of a behavioural recognition system in classrooms, this can lead to inequalities for children with autistic or hyperactivity disorders.

CREATION OF GHOST PROFILES

The use of facial recognition technologies can end up creating ghost profiles of people who do not use social media.

USES THAT COULD BE ACCEPTABLE TO CERTAIN CONTRIBUTORS

Some contributors advise that pain categorisation technologies can be useful in a variety of situations, such as for psychiatrists and care assistants in residential care homes, and on public transport (for people who suddenly feel unwell).

CNPEN 2 April 2021

Comité National Pilote d'Éthique du Numérique

Self-referral

Facial, posture and behavioural recognition: between questions and ethical issues

Artificial intelligence is harnessing the advances in software and the collection and use of big data to develop innovative technologies and applications that raise a host of new ethical issues.

These technologies include facial recognition, which analyses an individual's facial features for the purpose of confirming their identity, determining their emotions or revealing their ethnic origin, or even their sexual orientation or political opinions, and posture recognition, which identifies the distinctive features of their gait and generally their behaviour. They have spread so quickly that nobody has taken the time or trouble to address the ethical and epistemological issues that they raise.

These new technological possibilities, combined with strong social pressure stemming from a growing sense of insecurity, could easily lead to the temptation of believing that technology holds all the answers. The result would be constant surveillance of the entire population. Both the political motivations and the repercussions for civil liberties need to be examined with great care.

Looking beyond the model of society that could be shaped by these choices or non-choices, there is a need to address the issue of consent and debate with citizens, civil society stakeholders, legislators, economic players and politicians.

In recent years, we have seen several uses for facial, posture and behavioural recognition technologies emerge, with no absolute certainty that algorithmic quality will not lead to discriminatory biases. The current security and health climate is also acting as a considerable incentive. Several trials of the technology will soon be deployed at major events in France and abroad.

Some people are delighted to see applications that can improve human-machine interfaces, provide easier access to multimedia databases or ensure health safety (e.g. by spotting people not wearing a mask). Meanwhile, others are concerned about applications that could undermine civil liberties and anonymity. There are even people calling for a moratorium.

This referral will focus more specifically on the ethical implications of these technologies.

To carry out this analysis and distinguish between the various uses and applications, a distinction will be made between three scenarios:

1. Authentication

2. Identification

3. Categorisation

Authentication, i.e. comparing recorded biometric data against the data presented by an individual, is entering the mainstream with the possibilities offered by AI, which conjures up images of such traditional practices as fingerprinting. From a logical perspective, this is known as a *one-to-one* matching process. Authentication has long been used in airports, such as the PARAFE border control system, and the selfie check for automatic payment transactions, and unlocking phones and computer accounts. This system is generally based on cross-referencing several clues, typically with the individual's consent.

Identification, which involves identifying an individual in a crowd, could lead to a society where people are controlled without their knowledge due to the widespread use of surveillance and monitoring systems. From a logical perspective, this is known as a *one-to-many* identification process. Identification does not necessarily imply that users have given their prior consent. There are many ethical and legal questions that surround the conditions for potentially using these systems to recognise people and their intentions from CCTV footage in car parks or airports. Can we use these technologies at the risk of keeping track of the movements and interactions of each and every one of us? Or should they be given an outright ban while prohibiting a number of useful applications, such as for carrying out court-ordered investigations?

Categorisation, which aims to classify individuals and their behaviour based on their face or posture, runs the risk of discriminating against individuals according to their appearance, sexual orientation, political opinions or even their ethnic origin. From a logical perspective, this involves dividing people into classes and is known as *one-to-many* classification. Categorisation establishes a correlation between their facial features or posture characteristics, and their emotions, activities, character, ethnic origin or sincerity in situations as specific as lie detection. These are probably extremely old physiognomic conceptions that are now being revived in the modern era. In addition to epistemological questions about the robustness of the experiments carried out in these areas, questions also need to be asked about the extent to which such applications are acceptable and the effects that they will have on society, the relationship between the State and its citizens, and so on.

For each scenario of generic applications, the Committee will seek to formulate and examine the limits and the conditions for their potential or observed uses with the aim of preserving individual dignity, the sense of justice and what is ethically acceptable for our society in terms of its values.

In addition to the scenarios for generic applications and their uses, the Committee will take a closer look at the data, particularly the biometric data used as inputs for categorisation systems, both for algorithmic learning and for recognition, as well as the collection, accessibility and circulation of these data.

The Committee will examine the role and legitimacy of the various stakeholders currently involved in designing these facial, posture and behavioural recognition technologies, as well as their widespread distribution and development. What safeguards should be implemented between the State, local authorities, companies and citizens to ensure that the usage conditions are ethically acceptable?

Finally, the Committee will extend its investigations to encompass the cultural, geopolitical and sovereignty issues associated with the control and use of these technologies.

The Committee aims to deliver its opinion by the end of 2021.

Rapporteurs: Karine Dognin-Sauze & Jean-Gabriel Ganascia.

The CNPEN was set up in December 2019 at the request of the Prime Minister and placed under the authority of the National Ethics Advisory Committee for Health and Life Sciences (CCNE). The Committee comprises leading figures from academia, industry and the institutional sector. Experts in digital technology, law, economics, philosophy, language, logic and medicine all contribute to discussions on the ethical issues that have become essential as a result of the development of digital technology, while helping inform public debate. Previous opinions issued by the CNPEN include the ethical implications of «autonomous» vehicles (May 2021), chatbots (September 2021) and, alongside the CCNE, the ethical issues surrounding the use of artificial intelligence for medical diagnosis (November 2022), and health data platforms (February 2023). More recently, the CNPEN has addressed the ethical issues of retroactive name changes in digital scientific documents (June 2023) and generative AI systems (June 2023).

MEMBERS OF THE CNPEN

Gilles Adda
Raja Chatila
Theodore Christakis
Laure Coulombel
Jean-François Delfraissy
Laurence Devillers
Karine Dognin-Sauze
Gilles Dowek
Valeria Faure-Muntian
Christine Froidevaux
Jean-Gabriel Ganascia
Eric Germain
Alexei Grinbaum
David Gruson
Emmanuel Hirsch
Jeany Jean-Baptiste
Claude Kirchner - directeur
Augustin Landier
Gwendal Le Grand
Claire Levallois-Barth
Caroline Martin
Tristan Nitot
Jérôme Perrin
Catherine Tessier
Serena Villata
Célia Zolynski

Layout : DSAF/DPSG/BAEC/Section Édition – February 2025.