CIVIL LIBERTIES AND ETHICS

JUNE 2020

FACIAL RECOGNITION: EMBODYING EUROPEAN VALUES

RENAISSANCE numerique

TABLE OF CONTENTS

KEY TAKEAWAYS

Facial recognition technologies: probabilistic tools that process sensitive data

- Facial recognition technologies are based on artificial intelligence methods that apply so-called *deep learning* techniques to the field of computer vision, enabling the recognition of faces in images (video or still) based on biometric data. In this way, they differ from behavioral or emotional recognition technologies, which are based, for example, on the analysis of hand movements, trembling, eye movements or facial muscles.

- The processing of biometric data is, in principle, prohibited within the European Union (EU). The use of biometric data makes facial recognition technologies highly sensitive. The use of these technologies should be limited to exceptional cases only, and an alternative should always be preferred.

- Facial recognition technologies include a wide variety of technologies. Not all uses (public or private, consented to by individuals or without their knowledge, in real time or deferred time, etc.) involve the same sensitivity and risk.

- Facial recognition technologies are not foolproof. Their systems can be subject to significant security breaches and some technologies can induce biases that can lead to racist, sexist or ageist discrimination.

- Beyond these technical shortcomings, some flaws may

also result from human intervention in the interpretation of the results of these probabilistic technologies. It is essential that the users of these technologies be trained in their operation.

- Any decision made in which facial recognition technology is involved is the result of a chain of events. Therefore, it is essential to ensure that the decisions at each step in the chain are explainable, right up to the human decision.

The legal framework surrounding facial recognition technologies in Europe is relatively comprehensive, but its application is fragmented and inefficient

- Within the EU, facial recognition technologies are relatively well framed legally, either by fundamental rights, or by various European (GDPR, Law Enforcement Directive) and national texts (*Loi Informatique et Libertés* for example in France) that complement them.

- However, this legal framework suffers from weaknesses in its application, making it inefficient.

- On the one hand, European regulations are applied in a variable manner from one member state to another, particularly in the domain of fundamental research. In addition, national regulatory authorities have disparate and insufficient human and financial resources to devote to proper implementation.

- On the other hand, this framework suffers from difficulties with respect to guaranteeing fundamental rights. In the absence of *a priori* verification, it is complex to ensure the consistency of facial recognition technologies with our fundamental rights. As for the analyses carried out *ex post* by the courts, these require that the matter be referred to a judge, as well as a considerable investment on the part of the applicant, particularly in terms of time and skills.

Faced with the predominance of the United States and in order to guarantee its citizens' fundamental rights and freedoms, the European Union needs a robust European standardization system for facial recognition technologies

- The U.S. National Institute for Standards and Technology (NIST) currently dominates the international market for the standardization of facial recognition technologies. The evaluation criteria established by the NIST are widely used worldwide, including in European tenders. However, these standards refer exclusively to technical criteria.

- In order to establish its digital sovereignty and protect the fundamental rights and freedoms of its citizens, the EU must define its own standards taking into account legal dimensions. When it comes to facial recognition technologies, the reliability of a system cannot be determined simply by its technical performance.

- As facial recognition technologies are evolving, their compliance with European standards must be regularly assessed, as well as the standards themselves.

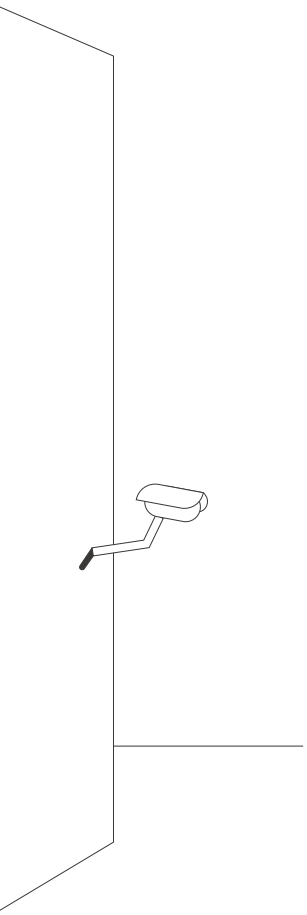
- The adoption of these standards must be achieved by imposing them in the context of European, national and local public procurement, including for trials. This obligation must guarantee their large-scale adoption through a performative effect.

- Beyond their adoption, the imposition of these standards in the context of public procurement should allow an effective framework for public surveillance.

- To achieve its standards, the EU must rely on a multi-stakeholder governance body, bringing together expertise in the fields of standardization and fundamental rights, including personal data protection, and, more generally, rights defense.

- The implementation of the European standardization system also requires investment (financial and human resources) from member states to strengthen the European supervisory authorities.

INTRODUCTION
THE FUNDAMENTAL GUARANTEES OF A DIGITAL SOCIETY



In its White Paper on Artificial Intelligence published last February, the European Commission announced its willingness to organize a broad debate on "*the collection and use of biometric data*[1] *for remote identification purposes*"[2]. In other words, the executive body of the European Union (EU) plans to initiate a dialogue on the subject of facial recognition technologies. According to the framework in force in the EU, the use of these relatively intrusive AI-based technologies should be limited to exceptional cases only. In accordance with Article 9 of the General Data Protection Regulation (GDPR)[3], the processing of biometric data for the purpose of "*uniquely identifying a natural person*" is in fact prohibited except in very specific cases: for example, if the individual concerned has given his or her explicit consent, or where such processing is necessary on the grounds of an overriding public interest[4]. Despite these restrictions, the experimentation and use of facial recognition technologies is spreading in several member states, hence the need for dialogue at the European and national levels.

1 In accordance with Article 3 §13 of Directive (EU) 2016/680 of 27 April 2016, Article 4 §14 of Regulation (EU) 2016/679 of 27 April 2016 and Article 3 §18 of Regulation (EU) 2018/1725 of 23 October 2018, *"'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data".*

2 European Commission (2020), "Artificial Intelligence: A European approach based on excellence and trust", Communication, COM(2020) 65 final, p. 22: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

3 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (hereinafter General Data Protection Regulation or "GDPR"), Article 9.

4 For the complete list, see Article 9(2) of the GDPR.

In recent years, facial recognition technologies have emerged in the daily life of French citizens in various forms: for border security under the PARAFE system[5], for unlocking smartphones and applications, for accessing secure facilities and for making online payments. Experiments using these technologies for security purposes have also been carried out, such as during the Nice carnival in March of 2019. Similar developments can be observed in most European countries. Although these technologies have reached a certain maturity and, in some cases, enable time efficiency, convenience and even security, their deployment and use, through their resort to biometric data, do have an impact on our fundamental rights and freedoms. This impact is all the more significant considering that a decision based on facial recognition technology can lead, for example, to the arrest and detention of an individual when these technologies are used for security purposes.

These issues are at the heart of the work of Renaissance Numérique, which defends the vision of a digital society that is inclusive and respectful of fundamental rights and freedoms. In line with this mission, the think tank remains vigilant with regard to digital devices that are intrusive and/or likely to restrict civil liberties. Although it is not based on facial recognition technologies as such, the testing of mask detection devices in the context of the current health crisis (in the city of Cannes[6] and at the Châtelet-Les Halles metro station in Paris[7]) demonstrates a trend that merits our concern. While having turnkey digital solutions to complex problems may seem attractive, we should not rush to adopt these tools before considering their potential negative effects on our rights and freedoms. The increasing frequency of these tests also highlights a social issue that goes far beyond facial recognition technologies: the use of intelligent video systems in public spaces. As a result of major technological progress (particularly in the field of artificial intelligence), devices designed to "make video surveillance systems intelligent" have been undergoing significant development for several years. In order to

5 The "*Passage automatisé rapide des frontières extérieures*" (PARAFE) system is based on the automated control of biometric passports, either through analysis of fingerprints or through the use of facial recognition technologies.

6 "À Cannes, des tests pour détecter automatiquement par caméras le port du masque", *Le Monde*, 28 April 2020: https://www.lemonde.fr/pixels/article/2020/04/28/a-cannes-des-tests-pour-detecter-automatiquement-par-cameras-le-port-du-masque_6038025_4408996.html

7 "La détection automatique du port du masque testée dans le métro parisien", *Le Parisien*, 8 May 2020: http://www.leparisien.fr/high-tech/la-detection-automatique-du-port-du-masque-testee-dans-le-metro-parisien-08-05-2020-8313348.php

enforce the confinement measures as part of the fight against Covid-19, the Paris police prefecture has used drones to monitor the population. On May 5, 2020, the Paris Administrative Court rejected a legal action filed by the Ligue des droits de l'Homme (LDH) and La Quadrature du Net against this use which, according to the plaintiffs, constitutes an infringement of the right to privacy and of the right to personal data protection[8]. Both organisations have appealed this decision. On May 18, the *Conseil d'État* ruled in favor of the two organizations, concluding that such a deployment, without the prior application of a regulatory text and without the opinion of the French Data Protection Authority *(Commission nationale de l'informatique et des libertés* - CNIL) constituted "*a serious and manifestly illegal violation of the right to privacy*"[9]. In a similar manner, the current interrogations around the regulation of facial recognition technologies is rekindling a debate on the balance between multiple fundamental freedoms. It is therefore necessary to take the time for informed collective reflection.

To contribute to this reflection, Renaissance Numérique has launched a working group in the fall of 2019, bringing together a dozen of experts - researchers, jurists and industry representatives[10]. This diversity of actors has enabled the think tank to address the issues related to facial recognition technologies not only from a technical perspective, but also from a legal and geopolitical angle. The working group produced an inventory of the relevant technologies and the legislative measures surrounding them at the national and European level. In addition to this internal process, the think tank also solicited various stakeholders willing to provide feedback on the subject through a series of hearings[11] and organized a symposium at the National Assembly in collaboration with Jean-Michel Mis, Deputy for the Loire region. Several dozen key actors from across the public sector, private sector, and civil society have contributed to the reflections presented here. In our commitment to put the general interest and citizens at the heart of the debate, Renaissance Numérique has also conducted, in partnership with the Ifop Institute, an opinion survey[12] on how French citizens perceive facial recognition technologies. This snapshot at a moment in time confirmed the need to gain perspective on the subject. Indeed, only 18% of those surveyed believe that they are sufficiently well informed about these technologies to have a precise opinion on how they should be used in society[13]. According to the interviewees, the use of these systems is mainly in relation to public security: in response to an open-ended question, the interviewees highlighted security-related uses and associated these systems most often with relatively alarming use cases involving surveillance. However, these uses are only part of the equation. Before embarking on any reflection, it is therefore necessary to clearly define what constitutes facial recognition technologies.

Concretely, the facial recognition technologies currently under development are based on artificial intelligence methods that apply so-called *deep learning* techniques to the field of computer vision, making it possible to recognize faces in images (video or static) based on biometric data. Contrary to some preconceived ideas, it is not possible to analyze the sensations or emotions felt by an individual using these technologies. In this respect, they differ from behavioral or emotional recognition technologies, which are based on the analysis of hand movement, tremors, eye movement, or facial muscles. As such, the latter are beyond the scope of the present reflection, although the possibility of pairing behavioral analysis systems with facial recognition technologies raises additional questions which must not be ignored. Facial recognition technologies should not either be confused with face detection, which is another aspect of computer vision, but which does not make it *de facto* possible to associate faces and individuals. Also, it is important to remember that not every video surveillance system is necessarily equipped with facial recognition technology.

8 "À Paris, la justice valide la surveillance du confinement par drones policiers", *Le Monde*, 6 May 2020: https://www.lemonde.fr/pixels/article/2020/05/06/a-paris-la-justice-valide-la-surveillance-du-confinement-par-drones-policiers_6038884_4408996.html ; "Confinement : la surveillance policière par drones dénoncée par deux associations", *Le Monde,* 4 May 2020: https://www.lemonde.fr/pixels/article/2020/05/04/confinement-la-surveillance-policiere-par-drones-denoncee-par-deux-associations_6038640_4408996.html

9 Conseil d'État (18 May 2020), n°s 440442, 440445: https://www.conseil-etat.fr/ressources/decisions-contentieuses/dernieres-decisions-importantes/conseil-d-etat-18-mai-2020-surveillance-par-drones

10 For the full list of experts who make up the Working Group, see the "The Working Group" section of this report.

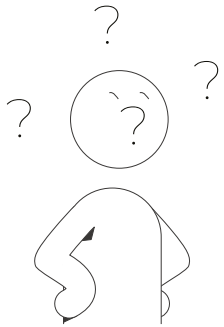
11 For a list of those interviewed, see the "Acknowledgements" section of this report.

12 The survey, carried out on a sample of 2007 people, is intended to be representative of the French population aged 18 and over.

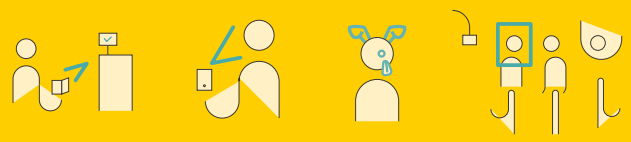
13 For an analysis of this survey, see Renaissance Numérique (2019), "Reconnaissance faciale : Ce que nous en disent les Français", 6 pp.: https://www.renaissancenumerique.org/ckeditor_assets/attachments/444/rn-analyse-reconnaissancefaciale.pdf

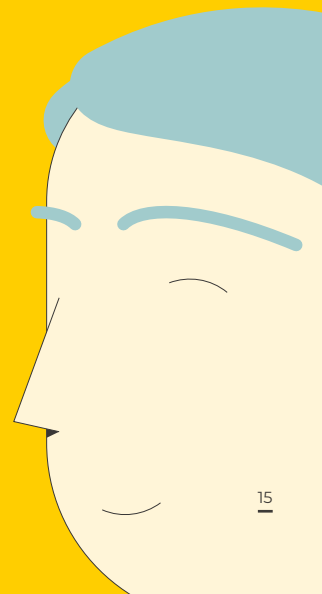
Importantly, the think tank has chosen to analyse the spectrum of facial recognition technologies in all its diversity, rather than simply "facial recognition" as a uniform concept. Approaching facial recognition as a one-dimensional technology would be meaningless, as the forms and uses of the technologies in question are numerous. Moreover, not all applications (public or private, consented to by individuals or without their knowledge, in real time or deferred time, etc.) involve the same sensitivity and risk. This brings us to question the adequacy of the regulatory framework surrounding these different uses. Is the current legal framework sufficient? Should it be supplemented by distinguishing between the various applications to render it more protective?

Because the deployment of facial recognition technologies in Europe mainly follows American standards, these issues should also be approached from an international perspective. The predominance of the United States in this area raises questions around digital sovereignty, which are all the more important since the sensitive personal data of European citizens are at stake. Examining the international framework in which these technologies are deployed highlights two fundamental challenges for the European Union: not only in establishing its technological independence, but also in developing technologies that are in line with its values. As has been the case in the area of personal data protection with the advent of the GDPR, the EU today has the opportunity to address these issues in order to ensure the protection of its citizens.



PART 1
THE TECHNICAL MATURITY OF FACIAL RECOGNITION TECHNOLOGIES PAVES THE WAY FOR THEIR DEPLOYMENT





A MATURITY IN LINE WITH THE DYNAMICS OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES

Research on artificial intelligence encompasses a wide range of both primary and applied research. The term "intelligence" evokes the idea of autonomous decision-making systems and can therefore feed into fantasies that critical decisions are made without the consent of human operators. However, facial recognition technologies essentially concern information processing that is simple to perform for a biological brain, but complex to automate on machines.

More specifically, facial recognition technologies are based on an application of mathematical and computational techniques developed in the field of computer vision, a branch of artificial intelligence. Today, these techniques are studied through the approach of *machine learning*, a field at the intersection of artificial intelligence and data science. Most often, this learning is supervised: an algorithm trains a statistical model to recognize faces in images from a massive volume of annotated data (*big data*).

Recent research into facial recognition draws on relatively mature *deep learning* techniques (see the box on "Deep learning"). Previously, pre-deep learning techniques had taken more than twenty years to increase accuracy from 60% to 90% on the benchmark *Labeled faces in the wild* (LFW)[14], a reference tool used for conducting work on facial recognition. The "deep" facial recognition techniques now in use, which apply multiple cascading layers of image processing in order to extract and transform physical features, have revolutionized the field since Facebook designed the Deepface[15] facial recognition system in 2014. Deepface achieved an unprecedented accuracy of 97% on the LFW benchmark. By way of comparison, even the best pre-professional learning techniques currently do not exceed 95% of accuracy[16]. Inspired by the remarkable performance of deep learning techniques, the state of the art systems (Deepface, DeepID series[17], VGGFace[18], FaceNet[19] and VGGFace2[20]) have relied on deep convolutional neural network architectures[21] to push LFW accuracy to 99.8% in just three years (in other words, the error rate has been divided by 15 in comparison to Deepface).

These results, emerging from both academic and industrial actors, are often published in conference proceedings or peer-reviewed scientific journals. The source codes of the trained algorithms and models are also very often open (open access in open source), which tends to encourage the deployment of these technologies.

14 The dataset *Labeled faces in the wild* contains more than 13,000 annotated facial photographs covering conditions typically encountered in real life: diversity of poses, lighting, focus, facial expressions, ages, genders, ethnicity, props, makeup, obstructions, backgrounds and quality. See: Gary B. Huang, Manu Ramesh, Tamara Berg and Erik Learned-Miller (2007), "Labeled faces in the wild: A database for studying face recognition in unconstrained environments", Technical Report 07-49, University of Massachusetts, Amherst, 11pp.

15 Yaniv Taigman, Ming Yang, Marc'Aurelio Ranzato and Lior Wolf (2014), "Deepface: Closing the gap to human-level performance in face verification", *CVPR*, pp. 1701-1708.

16 Mei Wang and Weihong Deng (2018), "Deep face recognition: A survey", 26 pp.

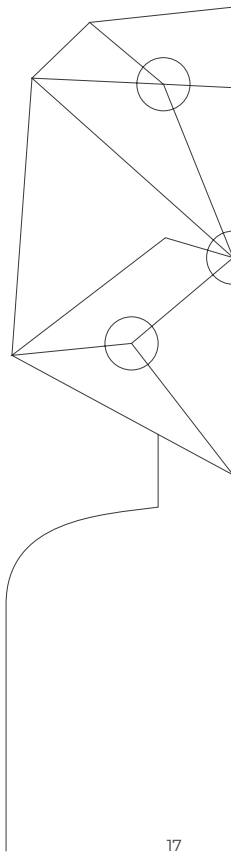
17 See: Yi Sun, Xiaogang Wang and Xiaoou Tang (2014), "Deep learning face representation from predicting 10,000 classes", *CVPR*, pp. 1891-1898 ; Yi Sun, Xiaogang Wang et Xiaoou Tang (2008), "Deeply learned face representations are sparse, selective, and robust", *perception*, 31:411-438 ; Yi Sun, Yuheng Chen, Xiaogang Wang and Xiaoou Tang (2014), "Deep learning face representation by joint identification-verification", *NIPS*, pp. 1988-1996 ; Yi Sun, Ding Liang, Xiaogang Wang and Xiaoou Tang (2015), "Deepid3: Face recognition with very deep neural networks", 5pp.

18 Omkar M. Parkhi, Andrea Vedaldi and Andrew Zisserman (2015), "Deep face recognition", *BMVC*, volume 1, p. 6.

19 Florian Schroff, Dmitry Kalenichenko and James Philbin (2015), "Facenet: A unified embedding for face recognition and clustering", *CVPR*, pp. 815-823.

20 Qiong Cao, Li Shen, Weidi Xie, Omkar M. Parkhi and Andrew Zisserman (2017), "Vggface2: A dataset for recognising faces across pose and age", 10 pp.

21 An artificial convolutional neural network is a type of artificial neural network in which neurons are connected so as to calculate mathematical operation of convolution in order to reproduce the biological process observed in the visual cortex of animals.

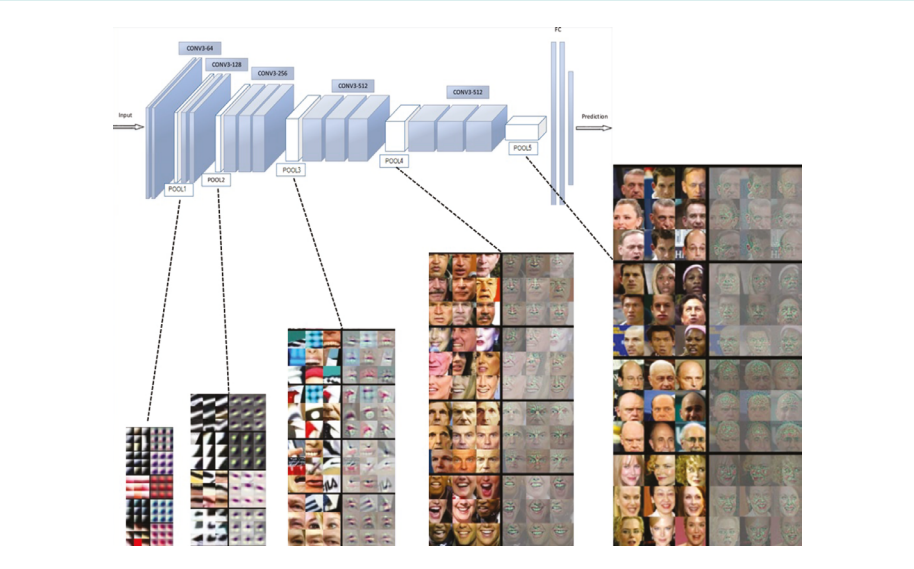


Deep Learning

Deep learning is based on the training of so-called *deep* artificial neural network models[22], whose breakthroughs in computer vision (notably in 2012 when the AlexNet system[23] won the ImageNet competition[24]) earned its developers the Turing Prize (equivalent to the Nobel Prize in Computer Science) in 2018. Deep learning is based on the biological process that leads a young child's brain to:

- learn to recognize familiar faces by observing faces in a variety of contexts;
- Quickly extract and memorize apparent physical characteristics relevant to different levels of abstraction (haircut, eye color, scarring, expression of emotion, wearing an accessory, etc.);
- associate them with people or groups of people;
- "generalize" the recognition of a face, i.e. recognize a face even in new contexts (with a new expression, colored lighting, change of position/orientation, new haircut, glasses, etc.).

22 Yann LeCun, Yoshua Bengio and Geoffrey Hinton (2015), "Deep learning", *Nature 521*, pp. 436-444.
23 Alex Krizhevsky, Ilya Sutskever and Geoffrey E. Hinton (2012), "Imagenet classification with deep convolutional neural networks", *Advances in neural information processing systems*, pp. 1097-1105.
24 Jia Deng, Wei Dong, Richard Socher, Li-Jia Li, Kai Li and Li Fei-Fei (2009), "ImageNet: A Large-Scale Hierarchical Image Database", *2009 conference on Computer Vision and Pattern Recognition*.



The above diagram[25] presents different invariances and abstractions learned by a network of convolutional artificial neurons trained to perform a facial recognition task. The first layer has learned to automatically recognize shapes that may be elementary but are nonetheless similar to those designed manually by human experts over decades. The second layer has learned to identify textures. The characteristics learned by the third layer are more complex: we observe eyes, mouths and noses. In the fourth layer, facial expressions are detectable such as a smile or frowning eyebrows. Finally, the last layer combines the features from the previous layers to produce a global representation (an abstraction) of the face that is supposed to encode enough information about the face to identify it with unprecedented stability.

25 This diagram is taken from Mei Wang and Weihong Deng (2018), *op. cit.*, p. 2.

THE FIELD OF FACIAL RECOGNITION ENCOMPASSES A DIVERSITY OF USES

The analysis of facial recognition must be considered in the plurality of its applications. Facial recognition tasks can be divided into two categories: verification (or authentication) and facial identification (or recognition).

VARIED USES WITH DIFFERENT LEVELS OF RISK

Face verification (or authentication) compares a given facial image to a known identity and answers the question "does this person appear in the image?" Verification, as an unlocking system (for example on smartphones), is a form of biometrics, similarly to fingerprint or iris recognition. Face identification (or recognition) associates a given facial image with an identity (or group of people) from a database of known faces. Identification answers the question "who is this person?". It can be applied as part of a system of monitoring or streamlining itineraries in the physical world (for example through customer tracking) or online. Face detection, which recognizes the presence of a face in an image and can potentially segment or track it if the system input is a sequence of images (for example a video), is often the first step of a verification or identification system. Its purpose is to align and standardize the faces contained in the images.

The three steps of biometric facial recognition

1) Enrolment phase

The first step is to capture data that is sufficiently representative of the diversity of the contexts in which the intended subjects will appear during the use of the technology. This corresponds to an image captured with little control, for example an image of moving people. Engineers can also rely on public databases. Learning models are trained from these databases.

2) Storage phase

A technology can centralize the photographs of users on a server, but users may prefer to have all their personal biometric data stored as close as possible to them, directly on their smartphones or on boarding passes if the application lends itself to this. This requires a comparison of the different levels of cybersecurity between storage methods.

3) Verification phase

The trained model returns an authentication score and the application decides whether this score is sufficient to conclude the verification (typically if the score exceeds a predefined threshold). The verification can take place on a server or as closely as possible to the sensor, storage system and/or user.

These tasks require recognition systems with different levels of accuracy, sensitivity and specificity[26] according to their applications and operating contexts: the performance of a model used for security purposes (border security, smartphone unlocking, online payment, access to public services) is thus more critical than that of a model dedicated to marketing (targeted advertising), which itself is more demanding than a recreational application (identification on photographs on a social network, *face swapping*).

26 "*In statistics, the sensitivity of a test measures its ability to give a positive result when a hypothesis is tested. This is in contrast to specificity, which measures the ability of a test to give a negative result when the hypothesis is not tested*". Definition from Wikipedia: https://en.wikipedia.org/wiki/Sensitivity_and_specificity

The *face swap* experiment

Developed by Snapchat since 2016, the *face swap* application allows users to exchange faces with their friends' on a photograph or a short video for recreational purposes. The deployment of *face swap* has generated considerable controversy, however, due to the risk of information manipulation:

- With regard to image misappropriation, *face swap* can be used to portray individuals in compromising situations, for example by tracing the faces of individuals on the bodies of actors to simulate the reproduction of pornographic images or videos. This type of image misuse, or *deepfake*, has prompted several responses from the pornography industry. The specialized platform Pornhub has prohibited the distribution of *deepfakes* and recalled the need to obtain the consent of individuals depicted in pornographic videos before distributing such content[27].
- With regard to the hijacking of speech, *face swap* allows the dynamic evolution of a face, for example to make an individual's mouth move and thereby lend him or her words that he or she did not say. In 2016, a video using *face swap* featured an Israeli leader threatening Pakistan. In response, the Defense Minister of Pakistan was led to hold a press conference to officially deny the existence of such a threat[28], which could have led Pakistan and Israel — both nuclear powers — to war.

The controversies linked to the use of *face swap* have not yet disappeared. The use of these technologies has been further enhanced by the software application Zao, which exacerbates the risk of information manipulation. In addition, the question of storing the collected facial data has been raised by many users in China, though no official answer has so far been given[29].

27 "Pornhub and Twitter ban AI-generated "deepfakes" videos that put female celebrities' faces on adult actresses" bodies", *The Independent*, 7 February 2018: https://www.independent.co.uk/life-style/gadgets-and-tech/pornhub-twitter-deepfakes-ban-ai-celebrity-faces-porn-actress-bodies-emma-watson-jennifer-lawrence-a8199131.html

28 "Experts fear face swapping tech could start an international showdown", *The Outline*, 1 February 2018: https://theoutline.com/post/3179/deepfake-videos-are-freaking-experts-out?zd=1&zi=4q34t-pv2

29 "Zao, l'application de vidéos «*deepfake*» qui inquiète les internautes chinois", *Le Figaro*, 2 September 2019: https://www.lefigaro.fr/secteur/high-tech/vie-privee-les-videos-deepfake-de-l-application-zao-inquietent-les-internautes-chinois-20190902

Highly sensitive uses, for example for security purposes, require extremely low error rates. A system deployed on the scale of the population of the European Union would have to achieve an error rate of 0.00000224% (i.e. an accuracy rate of 99.99999776%) to commit less than 10 errors for a total of 446 million individuals. We are still a long way from such performances.

When analyzing facial recognition technologies, the nature of the direct user must be accounted for, in addition to the technology's function. This could be, among others, an individual consenting by prior agreement using general conditions of use (or even operating conditions), a private company using facial identification for commercial purposes, or a public service seeking to monitor a population. In these last two cases, facial recognition can be applied without the knowledge of the targeted individuals and therefore identification carries with it risks to privacy. This is the case of several facial recognition devices currently being deployed and/or tested in France by government services for the purposes of the state:

- The Criminal Records Processing File (*traitement des antécédents judiciaires*, or TAJ) is notably used for the purposes of judicial or administrative investigations. Under articles 230-6 to 230-11 of the Code of Criminal Procedure[30], the TAJ includes photographs of persons who are the subject of a charge, investigation or inquiry for the purpose of ascertaining the cause of death, serious injury or disappearance. It includes technical features allowing the use of a facial recognition system. Given the particularly sensitive nature of this use (it may result in a criminal penalty or even imprisonment), data processing is carried out under the control of the public prosecutor with territorial jurisdiction. The latter may order the deletion of personal data that has been processed, for example in the event of an acquittal or termination of the investigation.

- The system for rapid and secure crossing of external borders (*passage rapide et sécurisé aux frontières extérieures*, or PARAFE) using facial recognition biometrics was introduced in 2018 to improve the fluidity of traffic. This allows passengers who consent to do so to cross the French

30 Articles created by Law No. 2011-267 of 14 March 2011, on guidance and programming for the performance of internal security.

border through an automated passport check[31] by means of a facial recognition device. According to Mathieu Rondel, Director of Expertise and Operational Performance at the ADP Group's Airport Operations Directorate, crossing the border using facial recognition would take 10 to 15 seconds, compared to 30 seconds using fingerprint recognition and 45 seconds using physical recognition by a border police officer[32]. Prior to its deployment for this purpose, the issue of protecting travelers' privacy has emerged as a major concern. When it was seized in 2016 on the draft decree aimed at authorizing these devices (the PARAFE automatic screening gates were until then based on fingerprint recognition), the CNIL reiterated its opposition to the creation of a central database that would make it possible to identify individuals[33]. According to the Commission, the use of biometric passports, which makes it possible to store the personal data of individuals in "*a format for the exclusive use of the individual*", is "*better able to ensure the protection of the privacy of individuals*"[34]. This recommendation is currently applied. The gates are also only accessible to individuals aged 12 and over and their use is optional, as the opportunity to report to a border police officer remains available. The existence of this alternative is viewed by the CNIL as an additional safeguard.

- Finally, the certified online authentication on mobile phones (*authentification en ligne certifiée sur mobile*, or ALICEM) is currently being tested in France as a way to access public services. This is an application developed by the Ministry of the Interior and the National Agency for Secure Documents (ANTS) that gives access to all partner services of FranceConnect, the State system that facilitates access to online services and has more than 500 public services available. When an individual creates an account on ALICEM, the photo contained on the chip of his or her identity document (passport or biometric residence permit) is extracted by a contactless reader. The individual is then asked to make a real-time video (in "selfie" style) and must perform three actions (smile, turn their head and blink, in random order). So-called "static" facial recognition is also carried out, using a photograph extracted from the video and compared with the photograph stored in the microchip. As with the two previous examples, this application raises questions in relation to the protection of personal data, to which the state is trying to respond. The Ministry of the Interior has made it known that users' personal data are only stored on their smartphones and are only used by ALICEM during the registration of the device[35]. The Ministry also stipulates that this data will not be used for any purposes other than electronic authentication and access to online services by ALICEM and that it will not be shared with third parties[36]. Seized for an opinion on the draft decree setting up the processing of biometric data as part of the development of the application, the CNIL – by deliberation on October 18th, 2018[37] – held that the implementation of this application must be conditional on the development of alternatives to facial recognition technologies, in order to ensure that individuals can consent freely to the processing of their biometric data during account activation.

31 Decree no. 2016-414 of 6 April 2016 modifying an automated processing of personal data known as "PARAFE".

32 Renaissance Numérique (2019), "Reconnaissance faciale : Interdiction, expérimentation, généralisation, réglementation. Où en est-on ? Où allons-nous ?", p. 19 : https://www.renaissancenumerique.org/publications/reconnaissance-faciale-interdiction-experimentation-generalisation-reglementation-ou-en-est-on-ou-allons-nous. See also the ADP Group's publication on Twitter, dated July 6, 2018: https://twitter.com/GroupeADP/status/1015124993729015808

33 Deliberation No. 2016-012 of 28 January 2016 delivering an opinion on a draft decree modifying the automated processing of personal data called PARAFE: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000032372514&categorieLien=id

34 *Ibid.*
Translated from the French original: "*un support dont la personne a l'usage exclusif [...] de nature à assurer une meilleure protection de la vie privée des personnes*".

35 Ministry of the Interior, "Alicem, la première solution d'identité numérique régalienne sécurisée", 16 December 2019 : https://www.interieur.gouv.fr/Actualites/L-actu-du-Ministere/Alicem-la-premiere-solution-d-identite-numerique-regalienne-securisee

36 *Ibid.*

37 Deliberation No. 2018-342 of 18 October, 2018, delivering an opinion on the draft decree authorising the creation of an automated processing system for authenticating a digital identity by electronic means known as the "*Application de lecture de l'identité d'un citoyen en mobilité*" (ALICEM) and amending the Code on the Entry and Residence of Foreigners and the Right of Asylum - request for opinion No. 18008244: https://www.legifrance.gouv.fr/jo_pdf.do?id=JORFTEXT000038475742

Facial recognition applied for international security purposes

China uses these technologies for social control and for the racial profiling of their Uighur population, in a policy of political surveillance.

In the United States, despite state-led initiatives to ban these technologies, facial recognition is used by federal agencies for national security purposes. In June 2019, the U.S. Congress highlighted in a report the efforts led by the FBI and the Justice Department to regulate the use of facial recognition technologies, following its previous recommendations issued in 2016. It regrets, however, that most of its recommendations have not been followed and insists on the need to update the guidelines on the protection of data collected by these technologies before launching pilot projects[38].

Singapore is securing Changi Airport with PARAFE-like devices that employ facial recognition technologies[39].

The United Kingdom is one of the only OECD member states to use facial recognition in public through the use of databases, without prior testing. The technologies deployed are based on the following operation: digital images of the faces of passers-by are taken from live video streams and processed in real time to extract facial biometric information. This information is then compared with facial biometric information of individuals on watch lists prepared specifically for each deployment.

38 United States Government Accountability Office (2019), "Face Recognition Technology: DOJ and FBI Have Taken Some Actions in Response to GAO Recommendations to Ensure Privacy and Accuracy, But Additional Work Remains", 23 pp.

39 "Singapore is introducing facial recognition at Tuas checkpoint. But there is one major drawback", *Mashable SE Asia*, April 2019: https://sea.mashable.com/tech/3231/singapore-is-introducing-facial-recognition-at-tuas-checkpoint-but-there-is-one-major-drawback

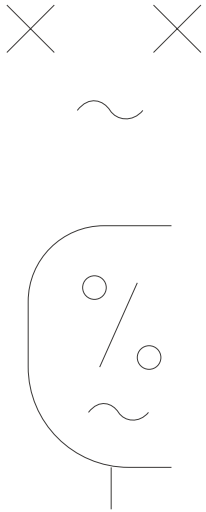
OVERLAP WITH OTHER TECHNOLOGIES RAISES FURTHER CONCERNS

The General Data Protection Regulation (GDPR) establishes the need to carry out a data protection impact assessment (DPIA), which is mandatory when processing operations aimed at uniquely identifying natural persons including so-called "vulnerable" populations (for example, students, elderly people, patients, asylum seekers, etc.).

Although there may be acceptable uses of facial recognition technology, a careful analysis of the context in which it is deployed can prevent the risks raised by its use in combination with other technologies in order to improve the identification and recognition of individuals. For example, a facial recognition system coupled with a fingerprint, iris or behavioral recognition system may increase or even create new risks of violating the consent of individuals and their right to privacy. Indeed, it is possible that the cross-referencing of various databases may generate new personal data without the users' consent.

Because the use of one application can lead to other uses, it is crucial to evaluate the technology and its impact not only at the time of initial deployment, but also over time, in order to assess future risks. This raises the question of liability when an application combines the technologies of multiple actors.

The metric used to measure the performance of algorithms is not absolute and must depend on the context in which an algorithm is used and its possible coupling with other biometric technologies: for example, a court decision on appeal may minimize Type I errors (false positives), while the early stages of a counter-terrorism investigation seek to reduce Type II errors (false negatives).



FACIAL RECOGNITION TECHNOLOGIES ARE NOT FOOLPROOF

THE INHERENT SHORTCOMINGS OF FACIAL RECOGNITION TECHNOLOGIES

The National Institute of Standards and Technology (NIST), an agency of the U.S. Department of Commerce responsible, among other things, for evaluating algorithms and defining standards, published Part 1 of the report "*Ongoing Face Recognition Vendor Test*" (FRVT) in 2018. This study compares the performance of 127 face identification algorithms submitted by 45 industrial and commercial research and development laboratories (including Germany's Cognitec, the American Microsoft, China's Yitu, France's IDEMIA, Japan's NEC and Russia's VisionLabs) and a university, based on a dataset of 26.6 million supervised facial images representing 12.3 million individuals. Despite different approaches and performances, the best algorithms in 2018 achieved error rates of less than 0.2%. Nevertheless, for at least 10% of the images, even if the identification was successful, the confidence rate[40] remains low and a human decision is still required to rule out the possibility that the proposed identity is a false positive.

40 The confidence level in an algorithmic prediction indicates the degree to which an algorithm is sure of the result it proposes. It is sometimes referred to as the "authentication score" for facial recognition and is usually expressed as a probability. *"For example, a face detection system may predict that an image region is a face at a confidence score of 90%, and another image region is a face at a confidence score of 60%."* (Amazon Web Services (2020), "Amazon Rekognition: Developer's Manual", p.126).

Image capture quality

Problems with image quality arise from the image capture system (the camera), the environment (light) or the presentation of the face to the capture system (orientation, blurring). Problems related to the image capture system and, to some extent, those caused by the environment, are external to facial recognition software technology and will undoubtedly be solved by better image capture and processing systems. These quality problems have been blamed for the very low positive predictive value (8%) observed when a facial recognition system was used during the 2017 Champions League final in Cardiff to detect the presence of suspected criminals[41].

The emergence and combination of efficient algorithms, powerful computing resources and massive annotated datasets have improved the performance of facial recognition to the point where these technologies are now available for practical and commercial use. We can reasonably expect to continue to see the error rate on specific datasets fall towards zero. Nevertheless, as the challenge of finding ideal conditions becomes obsolete (less optimal lighting, less adequate position, etc.), other challenges and problems will arise when these algorithms are taken out of research labs and integrated into routine applications.

First of all, it should be noted that face resemblance issues increase the error rate as the size of population under consideration increases: the rate is multiplied by 1.6 when considering a population of 12 million adults, compared to a population of 640,000 adults. In addition to look-alikes, the algorithms tested by the NIST are unable to distinguish between monozygotic ("identical") and dizygotic ("fraternal") twins. The U.S. agency report also mentions poor performance when it comes to identifying individuals over time. While systems have no difficulty recognizing an individual if they are presented with a photo of that individual who has aged two years (or "photo at +2 years"), the result is quite different if they are presented with a photo of the same individual who

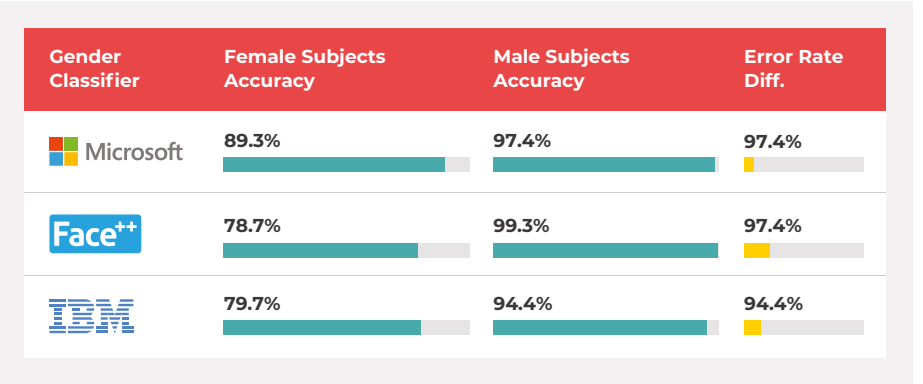
41 On this subject, see the site dedicated to automatic facial recognition devices developed by the *South Wales Police*: http://afr.south-wales.police.uk/

has aged eighteen years (or "photo at +18 years"). Even for the best system tested, the error rate for photos of adults who have aged 18 years is five times higher than that observed on photos of individuals who have aged only two years. Systems, especially those for time-sensitive forensic applications, must take into account age-related physical changes in individuals, but also the factors that can speed up these changes (like use of medication or drugs) or slow them down (like cosmetic surgery).

Worse still, studies have shown that some facial recognition technologies cause bias that can lead to racist, sexist or ageist discrimination. These biases come mainly from the data on which the learning models are trained. Indeed, public databases such as VGGFace2 (faces from Google Images) and MS-Celeb-1M[42] (celebrity faces) often come from websites and collect attractive photographs of young, smiling celebrities wearing makeup. These photographs poorly generalize the physiognomy of everyday populations. However, even a database created from images of daily life can show an uneven distribution of the different physical attributes of a population. First, a group (not necessarily a minority group) may be under-represented in this database because of a lack of representativeness in the creation of the database itself, for example if the database is generated from a sample where men outnumber women. However, even a database with a distribution faithful to that of the target population collects fewer examples representing a minority group than a majority group and may cause the models to produce a higher error rate on the minority group than on the majority group, resulting in bias and possible discrimination against one of the two groups, depending on the application. For example, IBM showed that among the databases most used to train facial recognition algorithms, over 80% of the LFW database contained photos of fair-skinned people.

This has prompted researchers to create more diverse datasets (such as *Racial Faces in-the-Wild*[43] (RFW)) to measure ethnic and gender biases in facial recognition algorithms. While not all studies on this subject are consensual (see the polemic on Amazon Rekognition between the American Civil Liberties Union[44] and Amazon[45]), we can cite the work of the *Gender Shades* project[46] led by researcher Joy Buolamwini at the Massachusetts Institute of Technology (MIT). This study created an annotated dataset and then tested facial recognition systems from Microsoft, IBM and Face++. The results are categorical: if the error rate of these three systems is less than 1% for light-skinned men, it reaches more than 20% for dark-skinned women.

FIGURE 1 - ERROR RATES OBSERVED ON MICROSOFT, IBM AND FACE++ FACIAL RECOGNITION SYSTEMS BY GENDER[47]



42 Yandong Guo, Lei Zhang, Yuxiao Hu, Xiaodong He and Jianfeng Gao (2016), "Ms-celeb-1m: A dataset and benchmark for large-scale face recognition", *ECCV*, pp. 87-102, *Springer*.
43 Mei Wang, Weihong Deng, Jiani Hu, Xunqiang Tao and Yaohai Huang (2018), "Racial faces in-the-wild: Reducing racial bias by deep unsupervised domain adaptation", 11pp.

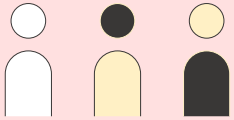
44 "Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots", *American Civil Liberties Union*, 26 July 2018: https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28
45 "Thoughts on Recent Research Paper and Associated Article on Amazon Rekognition", Amazon, *AWS Machine Learning Blog*, 26 January 2019: https://aws.amazon.com/fr/blogs/machine-learning/thoughts-on-recent-research-paper-and-associated-article-on-amazon-rekognition/
46 See the website: http://gendershades.org/ and Joy Buolamwini and Timnit Gebru (2018), "Gender shades: Intersectional accuracy disparities in commercial gender classification", *Conference on Fairness, Accountability and Transparency*, pp 77-91.
47 Source: http://gendershades.org/overview.html

These results are corroborated by an evaluation of 14 commercial facial recognition models on RFW that showed disparities in performance between different ethnic groups, with a 12% difference in error rate between the best and worst performing groups.

Media coverage of suspected discriminatory bias

In 2015, engineer Jacky Alciné publicized on Twitter an existing bias in Google Photo, which detected gorillas in a photograph showing two faces of people of color[48].

Apple's facial authentication system was also blamed in 2017 in an article in the *Sun*[49] for failing to differentiate between the faces of people of Asian origin as well as it does between the faces of Caucasian people.



Studies have also shown that despite very low error rates in sufficiently varied databases of faces, facial recognition systems are subject to significant security weaknesses. Presentation attacks[50] allow individuals to cover themselves (makeup, anti-pollution masks like during the 2019 demonstrations in Hong Kong, wigs, 3D silicone masks) to deceive the devices.

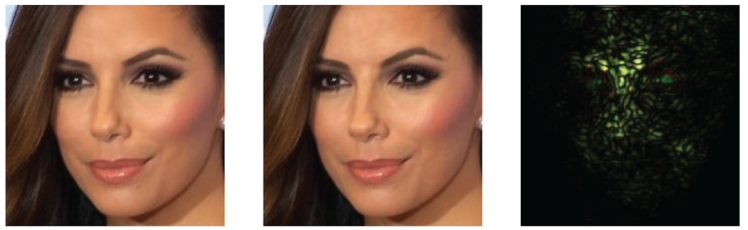
48 See: https://twitter.com/jackyalcine/status/615329515909156865

49 "Chinese users claim iPhoneX face recognition can't tell them apart", *The Sun*, December, 2017: https://www.thesun.co.uk/news/5182512/chinese-users-claim-iphonex-face-recognition-cant-tell-them-apart/

50 Raghavendra Ramachandra and Christoph Busch, "Presentation attack detection methods for face recognition systems: a comprehensive survey", *ACM Computing Surveys (CSUR)*, 50(1):8, 2017.

Dodging attacks

So-called "adversarial" attacks[51] rely on subtle, calculated variations in image pixels, often imperceptible to the naked eye, to change and distort the prediction of the algorithms. The image below is an example.



The photographs above[52] illustrate an example of an adversarial attack. On the left: original photograph of the actress Eva Longoria. Center: disturbed image of the actress. Right: filter that has disturbed the original image to create the disturbed image. An algorithm that correctly recognized the actress in the photograph on the left failed to recognize her in the disturbed image in the center, though the disturbance is imperceptible to the naked eye.

While some cyber-risks can be explained by the technical limitations of facial recognition, others stem from the predictive capacity of the algorithms. In addition, this predictive capacity can raise ethical concerns. A study pub-

51 Akhil Goel, Anirudh Singh, Akshay Agarwal, Mayank Vatsa and Richa Singh (2018), "Unravelling robustness of deep learning based face recognition against adversarial attacks", 8 pp ; Akhil Goel, Anirudh Singh, Akshay Agarwal, Mayank Vatsa et Richa Singh (2018), "Smartbox: Benchmarking adversarial detection and mitigation algorithms for face recognition", *IEEE BTAS*, 7 pp.

52 These photographs are taken from Mahmood Sharif, Sruti Bhagavatula, Lujo Bauer, Michael K. Reiter (2016), "Accessorize to a crime: Real and stealthy attacks on state-of-the-art face recognition", *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, pp. 1528-1540.

lished in *Nature Medicine*[53] proved that images of faces contain sufficient information for a powerful system to predict demographic and phenotypic information such as gender expression, age or private and particularly sensitive genetic information (family ties, ethnic origins). In the same vein, a research team at Stanford University[54] has shown that an algorithm trained to classify the sexual orientation of women and men simply on the basis of facial characteristics can predict the sexual orientation of individuals with an accuracy of over 83%, whereas humans are only 61% accurate. This study concludes by discussing the dangers of facial recognition on the privacy and security of LGBTQ+ people. It is therefore necessary to reflect on safeguards for the confidentiality of this biological data and to prevent possible leaks. As Raphaël de Cormis, Vice President of Innovation and Digital Transformation at Thales, points out, "*the larger the data, the more the size of the honeypot can attract attackers and put users at risk*"[55]. It is therefore necessary to avoid the centralization of data.

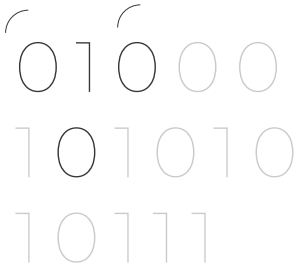
According to the NIST report, the revolution in deep learning explains the strong performance improvements over the period of 2013-2018 compared to between 2010-2013. Convolutional artificial neural network models benefit from a high robustness to invariance and work to resolve limitations due to unsupervised presentation of faces in front of camera lenses. However, these deep learning technologies are not immune from producing discriminatory biases. Their "black-box" aspect complicates their ability to be audited: it is impossible to predict the exact behavior of a technology of this nature from the moment it is designed. As a consequence, facial recognition providers must ensure the transparency of the performance of their models on different groups of people.

53 Yaron Gurovich, Yair Hanani, Omri Bar et al. (2019), "Identifying facial phenotypes of genetic disorders using deep learning", *Nature Medicine*, 25:60 – 64.
54 Michal Kosinski and Yilun Wang (2018), "Deep neural networks are more accurate than humans at detecting sexual orientation from facial images", *Journal of Personality and Social Psychology*, Volume 114, Numéro 2, pp. 246-257.
55 Renaissance Numérique (2019), "Reconnaissance faciale : Interdiction, expérimentation, généralisation, réglementation. Où en est-on ? Où allons-nous ?", p. 34: https://www.renaissancenumerique.org/publications/reconnaissance-faciale-interdiction-experimentation-generalisation-reglementation-ou-en-est-on-ou-allons-nous

A PERPETUAL TECHNOLOGICAL RACE TO CORRECT THEIR NEGATIVE EFFECTS

The deep learning revolution in computer vision explains recent advances in facial recognition and its integration into recreational, commercial, industrial, forensic and security uses. Error rates on some databases continue to decrease (on average the error rate is halved every year). However, the annotated datasets that are used to train and evaluate models are not always sufficiently diverse and can lead to biases that will result in discrimination in their applications. The technological race therefore encourages actors to minimize bias, either by diversifying the training databases of the models (for example by inserting computer-generated images into them) or by improving the models themselves (for example by adapting their recognition capacities from majority groups to minority groups).

Despite these advances, the technological race to correct errors in facial recognition devices is endless. On the one hand, by definition these technologies can never be 100% reliable. On the other hand, cyber-attacks and decoy attacks are progressing in parallel with the progress made by the industry.

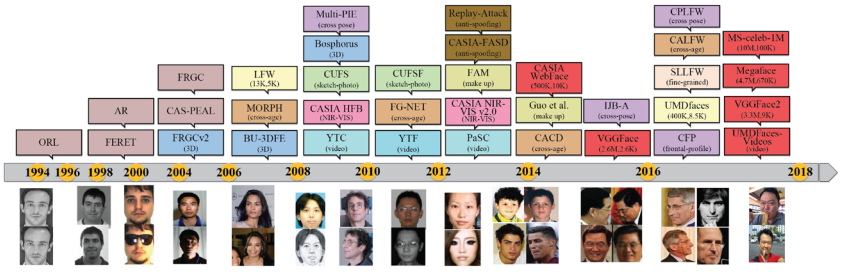


Increasingly unsupervised annotated facial image datasets

A supervised learning model requires a significant amount of annotated data to learn and generalize well. While initially the industry's deep facial recognition datasets were privately owned, other databases have been made public so that the academic community could catch up with industry research.

The figure below shows the evolution of the datasets used in facial recognition, with the effect of increasing scale and a generalization of images showing faces with less and less supervision and constraint: ages, poses and expressions vary, then external elements obscure certain parts of the faces, either by cropping them or putting makeup on them.

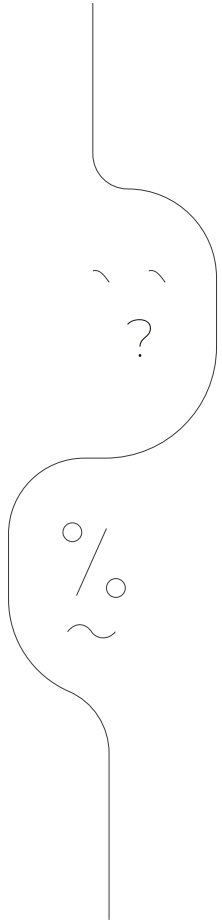
Evolution of facial recognition databases since 1994[56]



56 This diagram is taken from Mei Wang and Weihong Deng (2018), *op. cit.*, p. 13.

PROBABILISTIC TECHNOLOGIES PRONE TO HUMAN DEFICIENCIES

Beyond the technical shortcomings inherent in facial recognition technologies (errors, discriminatory biases, cyber-risks), some flaws may result from human intervention in the identification processes.



Public safety is a common case in which the final decision rests with human beings, and where the decisions at stake are likely to seriously affect the fundamental freedoms of individuals. When a video surveillance system at the entrance to a stadium or in the street identifies a person as a wanted criminal, this identification cannot automatically be considered valid. Because facial recognition is a probabilistic technology, the risk of false positives is far too high when it comes to the apprehension and arrest of an individual. Therefore, it is essential that security officers, and indeed users broadly, be trained in the operation of these probabilistic technologies and in the interpretation of the results they present. Every user must guard against "automation bias", or the idea of placing too much trust in the machine and ignoring external information that could contradict the results of the algorithm[57]. In order to minimize the risk of misjudgment when 'manually' checking a computer-generat-

57 For more on automation bias, see: https://en.wikipedia.org/wiki/Automation_bias

ed match, it is also essential to ensure that the confidence level of the result is as high as possible. For example, in its "*Developer Guide*" for its Rekognition product, Amazon advises law enforcement agencies to use a similarity threshold of 99% or above[58] to minimize the risk of misidentification. As indicated in the manual, a facial match established by a system such as Amazon Rekognition cannot constitute irrefutable proof of a person's identity, and must inevitably be corroborated by additional evidence (verification of identity documents, fingerprints, DNA, etc.).

Furthermore, it is important to bear in mind that any decision taken in which facial recognition technology is involved is the result of a chain of events. It is therefore essential to ensure that decisions at each level of the chain can be explained, right down to the human decision. Indeed, as the European Commission points out in its White Paper on Artificial Intelligence, "*opacity ("black box effect"), complexity, unpredictability and partially autonomous behaviour*" are characteristic of many AI technologies[59]. It is therefore not a question of explaining how these "black boxes" work, but rather of being able to identify the data that were used to make the system learn and explain the training approach of the system beforehand, along with the elements that led the system to a decision afterwards. Prior understanding should thus encourage the development of facial recognition technologies that are *ethical by design* (in other words, whose source code integrates ethical dimensions) and to identify possible biases inherent in these technologies from the design stage. Subsequently, it is a question of monitoring the results presented by the algorithms over time[60]. The evolutionary nature of these technologies makes it necessary to monitor the results regularly in order to be able to improve them[61].

At the same time, when an individual is deprived of his or her liberty as a result of a decision made with the help of a facial recognition device, this is not solely because of the machine. In applications where this technology is used as a decision aid, it is also necessary to account for the human biases which persist regardless of the level of confidence in the equipment. In addition, it should be the responsibility of the provider of the facial recognition technology to explain to its customer (for example, law enforcement) the precise functioning of the device and how the results of the technology should be taken into account in its decision. Consideration should also always be given to less intrusive alternatives.

> Despite significant technological advances made possible by the use of deep learning in recent years, facial recognition technologies remain not only imperfect but also highly sensitive devices. The processing of biometric data is far from being a trivial activity and the risk of violation of our fundamental rights and freedoms merits particular attention. However, the number of relatively sensitive uses and experiments is increasing, including in several member states of the European Union. It is therefore necessary to wonder whether the legal framework surrounding them really is sufficient to prevent applications of facial recognition technologies that could jeopardize our fundamental rights.

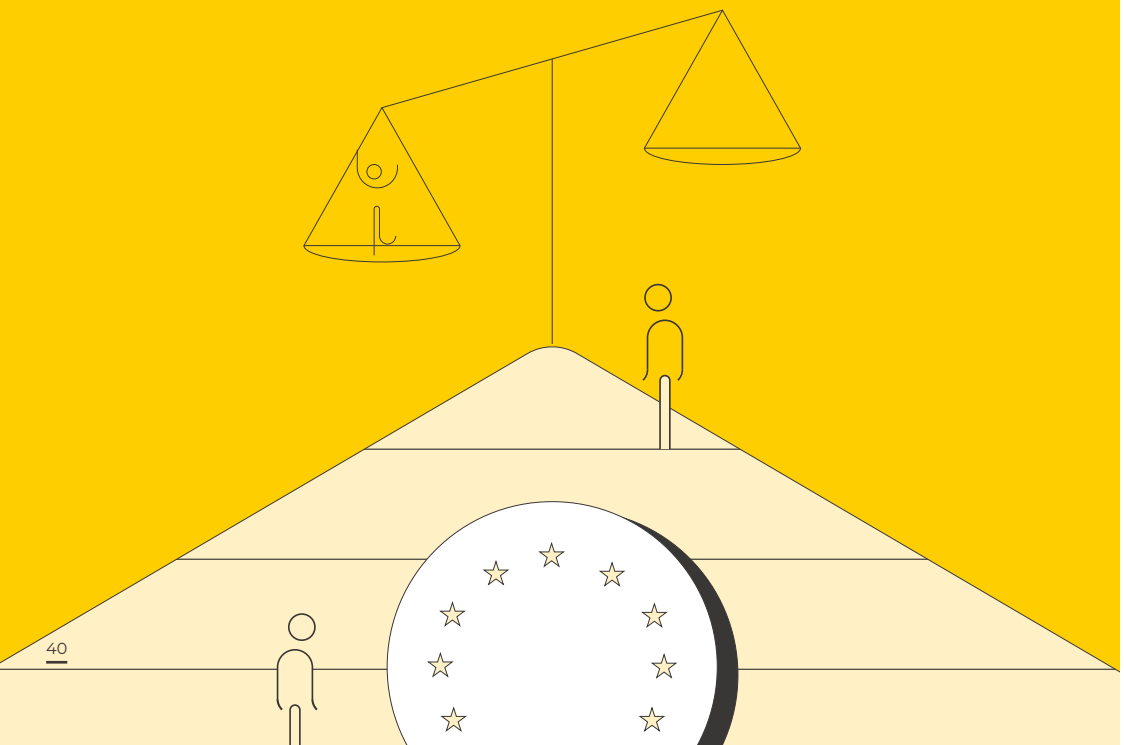
58 Amazon Web Services (2020), *Ibid.*, p.155: https://docs.aws.amazon.com/rekognition/latest/dg/rekognition-dg.pdf

59 European Commission (2020), "Artificial Intelligence: A European approach based on excellence and trust", Communication, COM(2020) 65 final, p. 12: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

60 On this subject, see Renaissance Numérique (2017), "L'éthique dans l'emploi à l'ère de l'intelligence artificielle", 23 pp.: https://www.renaissancenumerique.org/system/attach_files/files/000/000/137/original/Renaissance_Nume%CC%81rique_IA___Emploi_Oct2017.pdf?1508946963

61 *Ibid.*, pp. 20-21.

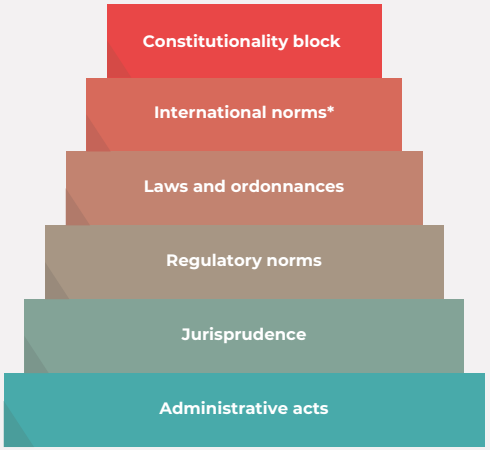
PART 2
AN INCONSISTENT AND INEFFICIENT APPLICATION OF THE LEGAL FRAMEWORK



FACIAL RECOGNITION TECHNOLOGIES ARE RELATIVELY WELL REGULATED

Whether in France, within the European Union or at the international level, the development of facial recognition technologies does not take place in a total legal vacuum. This development is framed by numerous standards at various levels, ranging from fundamental rights and freedoms to national legislations. In order to analyze the legal framework applicable to facial recognition technologies, it is therefore necessary to consider the entire existing normative framework and to begin with the highest norms, in particular the fundamental rights and principles that are the foundation of democracies, before looking at inferior norms.

FIGURE 2 - THE HIERARCHY OF NORMS



*subject to ratification by States and inclusion in their norm-setting system

FUNDAMENTAL RIGHTS ARE APPLICABLE TO FACIAL RECOGNITION TECHNOLOGIES

Fundamental rights form the basis of democracies. As such, they also represent the highest standards for facial recognition technologies. At the international level, many texts guarantee fundamental rights that may be impacted by the use of these technologies.

RIGHTS THAT ARE GUARANTEED WIDELY

In this regard, the 1948 Universal Declaration of Human Rights[62] goes so far as to directly link fundamental rights to world peace: "*recognition of the inherent dignity and of the equal and inalienable rights of all members of the human family is the foundation of freedom, justice and peace in the world*". This Declaration is supplemented at the international level by specific texts that specify and refine certain rights and principles contained in the Declaration. These include, among others, the International Covenant on Civil and Political Rights[63], the International Covenant on Economic, Social and Cultural Rights[64] and the Convention on the Rights of the Child[65]. The application of these international texts depends essentially on their ratification by States, the absence of reservations, and their adoption at the national level (through amending the Constitution, for example).

Furthermore, the principles contained in the Universal Declaration of Human Rights have found further legal scope through the adoption of binding regional texts. Such is the case with the European Convention for the Protection of Human Rights and Fundamental Freedoms[66] which was signed within the Council of Europe on November 4, 1950 and entered into force in 1953. The European Court of Human Rights, seated in Strasbourg since 1959, monitors its application by member countries and the respect for the rights it guarantees. Within the European Union, the Treaty of Lisbon, which entered into force on December 1st, 2009, conferred on the Charter of Fundamental Rights of the European Union[67] the same legal force as the Treaties of the European Union. It is consequently binding on member states, and any citizen can invoke it when his or her rights are not respected. It is based on the principle of democracy and the rule of law.

In France and within the EU – democracies that share the values of the Universal Declaration of Human Rights, the European Convention on Human Rights, and have given a higher value to the Charter of Fundamental Rights – the design, development and deployment of facial recognition technologies must be analyzed legally within this normative framework.

THE FUNDAMENTAL RIGHTS LIKELY TO BE AFFECTED BY THE USE OF FACIAL RECOGNITION TECHNOLOGIES

Facial recognition technologies challenge many of the fundamental rights enshrined in the above-mentioned texts.

The European Union Agency for Fundamental Rights (FRA) carried out a detailed review of the use of facial recognition technologies by public authorities in a note published in November 2019[68]. In this report, the Agency underlines the following rights:

- human dignity;
- privacy;
- protection of personal data;
- non-discrimination;
- the rights of the child and the elderly;

62 United Nations (1948), Universal Declaration of Human Rights: https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf
63 United Nations (1966), International Covenant on Civil and Political Rights: https://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx
64 United Nations (1966), International Covenant on Economic, Social and Cultural Rights: https://www.ohchr.org/EN/ProfessionalInterest/Pages/CESCR.aspx
65 United Nations (1989), Convention on the Rights of the Child: https://www.ohchr.org/EN/ProfessionalInterest/Pages/CRC.aspx
66 Council of Europe (1950), European Convention for the Protection of Human Rights and Fundamental Freedoms: https://www.echr.coe.int/Documents/Convention_ENG.pdf

67 European Union (2000), Charter of Fundamental Rights of the European Union: https://www.europarl.europa.eu/charter/pdf/text_en.pdf
68 European Union Agency for Fundamental Rights (2019), "Facial recognition technology: fundamental rights considerations in the context of law enforcement", 36 pp.: https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law

- the rights of persons with disabilities;
- freedom of assembly and association;
- freedom of expression;
- the right to good administration;
- the right to a fair trial.

TABLE 1 - EXAMPLES OF FUNDAMENTAL RIGHTS LIKELY TO BE AFFECTED BY THE USE OF FACIAL RECOGNITION TECHNOLOGIES

Fundamental rights or freedoms[69]	Impact of facial recognition technologies
Human dignity	Facial recognition technologies, especially when used in real-time, can be seen as surveillance technologies that are intrusive enough on people's lives to affect their ability to lead a dignified life.
Non-discrimination	Discrimination may occur in the design (conscious or unconscious) of the algorithm itself (through the introduction of bias) or as a result of the implementation, by those who decide what action to take based on the result of the algorithm.
Freedom of expression, association and assembly	The use of facial recognition technologies through video cameras installed in public space can deter people from expressing themselves freely, encourage them to change their behavior or revert to presenting them as part of a group of individuals. Some people may not want to gather in public spaces for fear of facial recognition technologies. This may also violate the freedom to remain anonymous.
The right to a fair trial	This right rests first and foremost on people's right to be informed. Thus, any lack of transparency could undermine this right[70]. In addition, public authorities must put in place procedures to enable the persons concerned to bring challenges and complaints. For example, individuals should be able to object to their inclusion in a matching database or claim compensation for damage due to misinterpretation of the results of facial recognition technologies.
The right to good administration	It refers to the concept of explicability and is based on a principle of transparency which implies that individuals may request to know the reasons why a decision has been taken against them. With regard to facial recognition technologies, this would mean that the administration or the police would have to be able to explain to a person the reasons why he or she has been arrested on the basis of the results of a facial recognition technology.
Right to education	A student who is denied access to a school in a region that has mandated access through facial recognition technologies, and does not offer any other access alternatives, may invoke his or her right to education.

69 The distinction between fundamental rights and fundamental freedoms stems from the fact that freedom is inherent in the person as an individual, whereas a right is an obligation that the State owes to individuals.

70 Informing people is an essential prerequisite. Without such information, recourse is not possible. See for example: CJEU (21 December 2016), cases C-203/15 & C-698/15, Tele2 Sverige AB v. Post-Och Telestyrelsen and Secretary of State for the Home Department v. Tom Watson and Others; CJEU (19 January 2010), Case C-555/07, Seda Kücükdeveci v. Swedex GmbH & Co KG.

Of course, certain uses of facial recognition technologies may raise issues regarding other fundamental rights. It is possible to imagine, for example, a ban on turning the human body and its parts into a source of profit, in the event that the capture of faces by facial recognition technologies is carried out for commercial purposes. Moreover, these rights are not exclusive: the use of facial recognition technology may call into question respect for multiple fundamental rights.

In France, concerning the protection of personal data and respect for privacy, Article 1 of Law 78-17 of 6 January 1978 on data processing, databases and liberties already provided that "*informatics must be at the service of every citizen. [...] It must not infringe on human identity, human rights, privacy or individual or public freedoms*"[71].

As indicated by the European Union Agency for Fundamental Rights, the impact in terms of fundamental rights varies considerably depending on the purpose, context and scope of the use of the facial recognition technology. Although some flaws arise from the lack of precision of the technology itself, some impacts persist even in the absence of error.

Most of the above-mentioned fundamental rights are not only guaranteed by the European Charter of Fundamental Rights, but also at international level. This means that the justification for the compatibility of facial recognition technologies with fundamental rights may also apply beyond the EU.

71 Translated from the French original: "*l'informatique doit* être *au service de chaque citoyen. [...] Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques*".

Internationally recognized principles

The **principle of non-discrimination** is internationally recognized: it is enshrined in Article 2 of the Universal Declaration of Human Rights. Several other rights derive from the principle of non-discrimination in order to protect vulnerable persons who are susceptible to particularly severe discrimination. These groups are afforded additional protection to ensure that equality of dignity and rights is achieved. This applies to children, the elderly and people with disabilities. The principle of racial non-discrimination also derives from this principle.

The **rights to an effective remedy and a fair trial** are also enshrined in articles 8 to 11 of the Universal Declaration of Human Rights. This means in particular that from the moment a person is arrested, the legitimacy of the arrest must be demonstrated.

Freedom of expression is a crucial right and another recognized foundation of democracy. It is enshrined in article 19 of the Universal Declaration of Human Rights and article 19 of the International Covenant on Civil and Political Rights.

The **freedoms of assembly and association** emanate from freedom of expression, but are also enshrined as such in the Universal Declaration of Human Rights (Article 20) and the Covenant on Civil and Political Rights (Articles 21 and 22).

HOW CAN FACIAL RECOGNITION TECHNOLOGIES BE RECONCILED WITH RESPECT FOR FUNDAMENTAL RIGHTS?

The question that then arises is how to reconcile these fundamental rights and principles with facial recognition technologies. The fact that facial recognition technologies have the potential to undermine these rights calls for the highest degree of caution.

This is particularly the case when it comes to human dignity, which is an "inviolable" right as stated in Article 1 of the European Charter of Fundamental Rights, meaning that it may not be infringed. Well before the adoption of the Charter of Fundamental Rights of the European Union, the French *Conseil d'État* had, in its famous "*Commune de Morsang-sur-Orge*" judgment of 27 October 1995, enshrined the principle of respect for human dignity as a component of public order (the so-called "dwarf throwing" affair); in this case, this principle prevails over the consent of the person him or herself. Similarly, the Constitutional Council has also considered that safeguarding human dignity is a principle with constitutional value and the Court of Justice of the European Union (CJEU) has recognized it as a general principle of law[72]. Therefore, if a facial recognition system violates human dignity then it must be banned, and no derogation from this rule is possible.

Though not possible with respect to human dignity (which cannot be derogated), it is possible under certain conditions to limit the exercise of other rights enshrined in the EU Charter of Fundamental Rights. Indeed, Article 52 of the Charter of Fundamental Rights of the European Union provides that "*any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others*."

It follows that any limitation on the rights enshrined in the Charter of Fundamental Rights of the European Union must:

- be provided for by law: in other words, fall within the scope of an existing text with current legal force;
- genuinely meet objectives of general interest recognized by the Union or of the need to protect the rights and freedoms of others;
- respect the essence of the rights and freedoms, in other words, the inalienable core of the right concerned;

72 Constitutional Council (27 July 1994), No. 94-343-344 DC; CJEU (14 October 2004), Omega, aff C-36/02.

- respect the principle of proportionality;
- be necessary (principle of necessity).

If the introduction of a facial recognition technology is likely to infringe a fundamental right and fails to meet one of these conditions, its deployment may be considered contrary to the Charter of Fundamental Rights of the European Union. It bears noting the CNIL's opinion on the draft decree relating to the "StopCovid" application, in which it reiterates the importance of compliance with the above-mentioned conditions, in particular the motive of general interest and the principle of proportionality[73].

The European Convention for the Protection of Human Rights and Fundamental Freedoms, while not as general in scope as the mechanism provided for in the Charter of Fundamental Rights of the European Union, also provides for a similar mechanism that applies to interference by public authorities in the exercise of certain rights enshrined in that Convention, namely the right to respect for private and family life, freedom of thought, conscience and religion, freedom of expression, freedom of assembly, association and movement. Interference by public authorities must therefore pursue certain aims defined by the convention and these must be "*necessary measures in a democratic society*"[74] and proportionate to the aim pursued.

The principle of proportionality is an essential concept. It is defined as "*a balancing mechanism between legal principles of equivalent rank, which are*

73 Deliberation no. 2020-056 of 25 May 2020 giving its opinion on a draft decree relating to the mobile application known as "StopCovid", §5 : "*La Commission rappelle néanmoins que les protections constitutionnelle et conventionnelle du droit au respect de la vie privée et à la protection des données à caractère personnel, assises notamment sur la Charte des droits fondamentaux de l'Union européenne et la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, imposent que les atteintes portées à ces droits par les autorités publiques soient non seulement justifiées par un motif d'intérêt général, comme cela est le cas en l'espèce, mais soient* également *nécessaires et proportionnées à la réalisation de cet objectif.*" ("*The Commission would nevertheless point out that the constitutional and conventional protection of the right to respect for private life and the protection of personal data, based in particular on the Charter of Fundamental Rights of the European Union and the European Convention for the Protection of Human Rights and Fundamental Freedoms, require that infringements of these rights by public authorities must not only be justified on grounds of general interest, as is the case here, but must also be necessary and proportionate to the achievement of that objective.*").

74 Council of Europe (1950), *op. cit.*

simultaneously applicable but contradictory[75]". It is a question of weighing up and striking a balance between each of the legal principles in question - generally a power conferred on the State (public order, law enforcement) and the fundamental rights of individuals - or between several fundamental rights. Respect for the principle of proportionality requires that a measure restricting rights and freedoms must be:

- appropriate, in that it must enable the legitimate objective pursued to be attained;
- necessary, in that it must not exceed what is required to achieve that objective;
- and proportionate, in that it must not, by the burdens it creates, be disproportionate to the result sought.

While the principle of proportionality was initially a mechanism used by judges to arbitrate between competing legal principles, this "triple test" has acquired a general application at the European level. Article 5 of the Treaty on European Union states that "*Under the principle of proportionality, the content and form of Union action shall not exceed what is necessary to achieve the objectives of the Treaties. The institutions of the Union shall apply the principle of proportionality as laid down in the Protocol on the application of the principles of subsidiarity and proportionality.*" The principle of proportionality is intended to limit and to frame the actions of the European Union, which must confine itself to what is necessary to achieve the objectives of the Treaties. This implies in particular that the European legislator must resort to this principle when adopting a text.

Originating in Germany, this "triple test" has gradually spread throughout Europe[76], including the United Kingdom. There is also emerging application

75 G. Xynopoulos, "Proportionnalité", in D. Alland and S. Rials (2003), *Dictionnaire de la culture juridique*, PUF, 2003, p. 1251.
76 CEDH (23 July 1968), aff. n° 1474/62, "Affaire relative à certains aspects du régime linguistique de l'enseignement en Belgique c. Belgique" pts. 5 et 10; CEDH (4 December 2008), aff. 30562/04 & 30566/04 S. and Marper v. the United Kingdom, paras. 95-104; CJCE (24 July 2003), aff. C-280/00 Altmark; CJUE (8 April 2014), aff. C-293/12 & C-594/12, Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others.

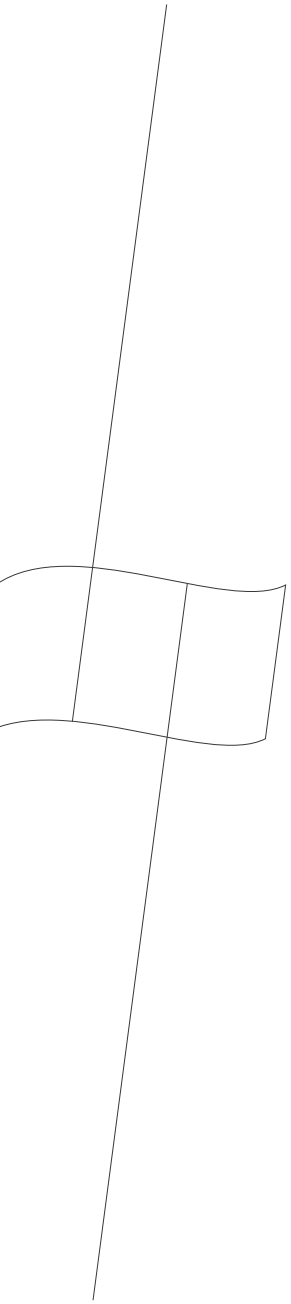
of the "triple test" in the United States[77]. In France, the Constitutional Council uses the proportionality test when monitoring legislative provisions that restrict the exercise of a right or freedom in the name of safeguarding public order, or when it has to reconcile multiple fundamental rights with one another[78]. The French Data Protection Authority *(Commission nationale de l'informatique et des libertés* - CNIL) regularly uses proportionality and necessity checks to verify the lawfulness of data processing. This is precisely what it did in its publication on facial recognition of November 15, 2019[79], as well as when it expressed its views on the application to locate individuals carrying Covid-19[80].

Full respect for fundamental rights is a precondition for any application of the law, whatever the technologies in question. It is therefore necessary to implement the "triple test" before any deployment of facial recognition technologies. Moreover, the more intrusive the technologies, the more strictly the test must be applied.

NATIONAL AND REGIONAL REGULATIONS COMPLETE THE FRAMEWORK OUTLINED BY FUNDAMENTAL RIGHTS

Beyond fundamental rights, which are at the top of the hierarchy of norms, the deployment of facial recognition technologies must also respect various national regulations that may apply. In order to inform the debate at the na-

77 United States Court of Appeals for the 9th District (9 February 2017), State of Washington v. Donald J. Trump et al, No. 17-35105. In this decision, the Court of Appeals weighed the decree's infringement of certain individual and state rights against the public interest in maintaining the decree.
78 Conseil constitutionnel (23 July 2015), n° 2015-713 DC, § 11; Conseil constitutionnel (22 December 2015), n° 2015-527 QPC, § 4; Conseil constitutionnel (10 February 2017), n° 2016-611 QPC.
79 "Reconnaissance faciale : pour un débat à la hauteur des enjeux", CNIL, 15 November 2019: https://www.cnil.fr/fr/reconnaissance-faciale-pour-un-debat-la-hauteur-des-enjeux
80 Hearing before the Laws Committee of the National Assembly, introductory remarks by Marie-Laure Denis, President of the CNIL, Wednesday 8 April 2020: *"Si un dispositif de suivi des personnes* était *mis en place de manière obligatoire, alors il nécessiterait une disposition législative et devrait, en tout* état *de cause, démontrer sa nécessité pour répondre à la crise sanitaire ainsi que sa proportionnalité en tenant compte des mêmes principes de protection de la vie privée, et en* étant *réellement provisoire". ("If an individual monitoring system were to be put in place on a mandatory basis, then it would require a legislative provision and would, in any case, have to demonstrate its necessity to respond to the health crisis as well as its proportionality, while taking into account the same principles of privacy protection, and remaining truly provisional".).*



tional and European level, it is necessary, in addition to the French and EU regulatory framework, to also observe the developments taking place abroad, particularly in the United States and China. This global dimension is all the more important since these two countries are trying to impose their standards in the global market for facial recognition technologies[81].

Before examining these regulations, it is interesting to note that these technologies have long been the subject of legal definitions:

- According to the "Article 29 Working Party" (now the European Data Protection Committee or "EDPB"), "*facial recognition is the automatic processing of digital images which contain the faces of persons for the purpose of identification, authentication/ verification or categorisation of those persons*"[82];
- According to the French CNIL, "*facial recognition is a programming and probabilistic technique that makes it possible to automatically recognize a person on the basis of his or her face, in order to authenticate or identify him or her*"[83].

81 "How the US plans to crack down on Chinese facial recognition tech used to 'strengthen authoritarian governments' ", *This Week in Asia*, 18 June 2019.
82 Opinion 02/2012 on facial recognition for online and mobile services, 22 March 2012.
83 "Reconnaissance faciale pour un débat à la hauteur des enjeux", CNIL, 15 November 2019.
In the original French, "*la reconnaissance faciale est une technique informatique et probabiliste qui permet de reconnaître automatiquement une personne sur la base de son visage, pour l'authentifier ou l'identifier*".

THE FRAMEWORK IN FRANCE

In France, facial recognition technologies are not regulated by a specific text. They are, however, subject to the regulations applicable to the processing of personal data and, to a certain extent, to the regulations applicable to the installation of video protection equipment. It should also be noted that, depending on the ultimate use, the implementation of facial recognition technologies may raise questions about rights other than the right to personal data protection or to privacy. One example of this could be in the area of labor law, when these technologies are used to provide secure access to business premises.v

The regulation applicable to personal data

Personal data is any information relating to identified or identifiable natural persons[84]. There are special categories of personal data, known as "sensitive" data, which include biometric data[85]. This data is subject to a stricter legal regime than other data.

Because facial recognition technologies involve biometric data, they are therefore subject to the rules applicable to the processing of personal data, namely:

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation or "GDPR");
- Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal

84 GDPR, article 4 §1: "*personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*"
85 GDPR, article 4 §14.

offences or the execution of criminal penalties, and on the free movement of such data, ("Law Enforcement Directive" or LED); and

- Law n°78-17 of 6 January 1978 relating to data processing, files and individual liberties, in its modified version ("*Loi Informatique et Libertés*").

In France, texts authorizing the use of facial recognition technologies for the processing of personal data were adopted a long time ago. No less than five expressly authorize the use of facial recognition technologies, namely, the Criminal Records Processing File (TAJ), the rapid and secure crossing of external borders (PARAFE), the certified online authentication on mobile phones (*authentification en ligne certifiée sur mobile*, or ALICEM) and two temporary uses for experimental purposes (in several airfields and as part of a "hackathon"). Moreover, as these technologies are generally considered "suspect" in French law, there are over twenty texts establishing processing operations involving digitized images of individuals that expressly exclude or even prohibit the use of facial recognition technologies, acting as "safeguards".

The GDPR - which applies not only in France, but throughout the member states of the European Union - requires compliance with a certain number of principles that apply to any processing of personal data, including biometric data, and therefore necessarily to facial recognition technologies. These include:

- the principle of lawfulness: all data processing must be based on one of the "legal bases" referred to in the GDPR in order to be implemented;
- the principle of fair and transparent processing: the data subject must be informed of the existence of the processing operation and its purposes (this obligation is reinforced for minors through the use of appropriate and comprehensible terms);
- the purpose limitation principle: data must be collected for specified, explicit and legitimate purposes;
- the data minimization principle: data must be adequate, relevant and limited to what is necessary for the purposes;
- the principle of accuracy: data must be accurate and up to date.

Before the entry into force of the GDPR[86], biometric data was not regarded as "sensitive data", that is, as data that cannot, in principle, be processed. Biometric data were essentially covered by the CNIL's authorization application system. In France, persons wishing to implement personal data processing involving facial recognition technologies thus had to obtain prior authorization from the CNIL. These applications for authorization have given rise to several deliberations by the authority[87]. The processing of biometric data (and thus the use of facial recognition technologies) is, in principle, prohibited[88]. There are, however, a number of exceptions to this prohibition principle. With regard to biometric data, and therefore, necessarily, to facial recognition technologies, several exceptions are likely to apply:

- when the person concerned has given his or her explicit consent;
- where processing is necessary in order to protect vital interests;
- where processing is necessary on grounds of substantial public interest;
- where processing is necessary for scientific research purposes (in France, this is currently limited to public research).

Where the legal basis for processing is the explicit consent of the data subject, such consent must not only be free, specific, informed and unambiguous; it is only valid if the data subject is able to decline or to withdraw his or her consent without suffering any prejudice. It is therefore necessary to provide an alternative solution for the data subject who might refuse to give consent or decide to withdraw it at a later stage. The GDPR specifies that where the controller is a public authority, it is unlikely that consent has been given freely, as there is often a clear imbalance of power between the controller and the data subject[89].

86 Under Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
87 To our knowledge, fourteen deliberations have authorized the use of facial recognition technologies and five have refused it.
88 GDPR, Article 9.
89 GDPR, Recitals 42 and 43; Article 29 Working Party - Consent Guidelines within the meaning of Regulation 2016/679.

Prior consent and proportionality: the example of "virtual access control" in high schools in the PACA region

On 27 February 2020, the Administrative Court of Marseille handed down the first case law decision concerning facial recognition in France. The regional council of Provence-Alpes-Côte d'Azur (PACA) had begun experimenting with a so-called "virtual access control" system in two high schools, consisting of the installation of facial recognition gateways at the entrances to these schools. The PACA Region sought to legally justify the processing of biometric data by obtaining the prior consent of the high school students concerned. The Administrative Court of Marseille granted the request for annulment of the decision, noting in particular that "*whereas the target public is in a relationship of authority with regard to the heads of the public educational establishments concerned, the Region does not justify having provided sufficient guarantees in order to obtain the consent of high school students or their legal representatives for the collection of their personal data in a free and enlightened manner*"[90].

The CNIL had also been seized by the Provence-Alpes-Côte d'Azur Region regarding a request for advice on this experiment, which had previously been the subject of an impact assessment relating to data protection, the results of which had been communicated to the authority. Following its decision of 17 October 2019, the CNIL noted that facial recognition devices are particularly intrusive and present major risks of infringement of privacy and individual freedoms, particularly when it comes to minors. In the presence of less intrusive alternative means (for example, access control through the use of badges), the authority considered that the envisaged device was contrary to the main principles of proportionality and data minimization laid down in the GDPR.

90 In the French original, "*alors que le public visé se trouve dans une relation d'autorité à l'égard des responsables des* établissements *publics d'enseignement concernés, la Région ne justifie pas avoir prévu des garanties suffisantes afin d'obtenir des lycéens ou de leurs représentants légaux qu'ils donnent leur consentement à la collecte de leurs données personnelles de manière libre et éclairée*".

The GDPR also provides for the need to carry out a data protection impact assessment (DPIA) on processing operations of personal data that are likely to pose a high risk to the rights and freedoms of the data subjects. The use of facial recognition technologies should require the implementation of a DPIA, either because they constitute an operation defined by the CNIL for which a DPIA is mandatory, or because they meet one or more of the criteria set out in the guidelines of the "Article 29 Group"[91]. Among these criteria, the Group specifically addresses facial recognition technologies by evoking the criterion of innovative use and the application of new technological or organizational solutions[92]. If it appears that the level of residual risk remains high, the results of the DPIA must be communicated to the CNIL.

Like the GDPR, the Law Enforcement Directive (LED) applies not only in France, but across all European Union member states. If facial recognition technologies are used for security or prevention purposes, they are not covered by the GDPR, but rather by the Law Enforcement Directive. This directive is in a sense the "twin" of the GDPR and was adopted at the same time. It applies essentially to the processing of personal data for the purpose of the prevention, investigation, detection, investigation, prosecution or enforcement of criminal offences, including the protection and prevention of threats to public security.

Under the Law Enforcement Directive, the processing of biometric data is authorized under the conditions laid down in Article 10: "*Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union*

91 For example, systematic surveillance, collection of sensitive data or highly personal data, large-scale collection of personal data, cross-referencing of data, data concerning vulnerable persons (patients, the elderly, children, etc.) or innovative use (use of new technology).

92 Article 29 Data Protection Working Party (2017), 'Guidelines on data protection impact assessment (DPIA) and how to determine whether the processing is 'likely to create a high risk' for the purposes of Regulation (EU) 2016/679', p. 12: *"Innovative use or application of new technological or organizational solutions: for example, combined use of fingerprint and facial recognition systems to improve physical access control, etc."*.

membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be allowed only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and only:

(a) where authorised by Union or Member State law;

(b) to protect the vital interests of the data subject or of another natural person; or

(c) where such processing relates to data which are manifestly made public by the data subject."

Two conditions are therefore required *a minima* by the Law Enforcement Directive for the processing of biometric data: it is possible to process biometric data (1) only in cases of absolute necessity, subject to safeguards for the rights and freedoms of the data subjects and (2) only where such processing is authorized by the law of the Union or the law of a member state.

The notion of "absolute necessity" raises questions, because if another course is possible – which always seems to be the case[93] – this could amount to a total exclusion of the possibility of using biometric data and consequently facial recognition technologies. It is difficult to answer this question at the moment, as it has - as far as we know - not been settled by case-law. The CNIL, when asked for its opinion, does not address this concept directly, but more often focuses on the implementation of appropriate safeguards[94].

With regard to individual's consent, this cannot constitute a legal basis for the processing of data involving facial recognition technologies under the Law Enforcement Directive. The implementation of a system for security purposes requires at a minimum the adoption of a law or a decree by the *Conseil d'État*. However, in the case of a simple experiment, i.e. without going beyond testing, it falls within the scope of the GDPR and, ultimately, it will most often be necessary to obtain the consent of the volunteers.

Experimentation at the 2019 Nice Carnival: an incomplete report according to the CNIL

A surveillance device based on facial recognition technologies was tested for several days in the city of Nice during the March 2019 carnival. Nearly 1,000 people agreed to be identified within the crowd in real time by facial recognition technologies based on six cameras positioned within the test perimeter. The City of Nice has encountered legal challenges that have hampered experimentation and has expressed its wish to see French legislation evolve with regard to experimentation with new technologies in real conditions in public spaces (and more specifically the *Loi Informatique et Libertés*). The CNIL asked for additional information, in particular on algorithm error rates, image quality and the risks of discrimination, and found the City of Nice's report to be incomplete.

The *Loi Informatique et Libertés (LIL)* is, naturally, aligned with the logic laid down in the European texts. Its Article 6 refers to the exceptions provided for in the GDPR concerning the processing of biometric data[95]. In fact, the GDPR allows the processing of biometric data in certain specific cases, for example for scientific research purposes, where it is necessary *"on the basis of Union law or the law of a Member State"*[96]. EU member states therefore have some flexibility: they can allow the processing of biometric data for scientific research purposes provided that they adopt specific texts. At present, however, the French legislature and the regulation authority have not adopted such texts. It is therefore not possible at present to process biometric data for sci-

93 For example, with regard to the use of facial recognition by police forces, it is always possible to use human labor, such as shadowing, rather than monitoring a mass of individuals by means of cameras installed in public spaces.

94 See for example: Deliberation No. 2019-123 of 3 October 2019 giving its opinion on a draft decree creating an automated processing of personal data called "mobile note-taking application" (GendNotes).

95 Loi Informatique et Libertés, Article 6.II: *"Les exceptions à l'interdiction mentionnée au I sont fixées dans les conditions prévues par le 2 de l'article 9 du règlement (UE) 2016/679 du 27 avril 2016 et par la présente loi".*

96 GDPR, article 9 §2 (j).

entific research purposes in France, with the exception of for public research purposes, as such processing is made possible by the *Loi Informatique et Libertés*[97].

If a text is necessary, the processing carried out on behalf of the State involving facial recognition technologies should also give rise to a reasoned opinion by the CNIL and a decree by the *Conseil d'État*[98].

Regulations pertaining to videoprotection

In France, in addition to the regulations applicable to personal data (GDPR, Law Enforcement Directive, *Loi Informatique et Liberté*), the use of facial recognition technologies is governed by the regulations on video protection. These regulations result essentially from articles L.251-1 and following of the Internal Security Code (CSI). It applies to the installation of collection devices on public thoroughfares and in places open to the public, excluding those installed in private places and workplaces not open to the public ("video surveillance"). Under these regulations, the installation of a video protection device must meet certain objectives determined by the legislator[99], notably:

- the protection of public buildings and public facilities and their surroundings;
- the safeguarding of facilities useful to national defense;
- the regulation of transportation flows;
- the detection of traffic violations;
- the prevention of attacks on the security of persons and property in places particularly exposed to risks of aggression, theft or drug trafficking, as well as the prevention of customs fraud, in areas particularly exposed to these offenses;
- the prevention of acts of terrorism;
- the prevention of natural or technological risks;
- the rescue of persons and defense against fire;
- the security of facilities open to the public in amusement parks;
- compliance with the obligation to be covered by insurance guaranteeing civil liability in order to operate a land motor vehicle.

Depending on the aims pursued, the installation of video protection systems also falls under the GDPR, the Law Enforcement Directive or the *Loi Informatique et Libertés*[100].

In addition, the regulations on video protection also require operators to:

- inform persons likely to be filmed by means of posters or signs (the obligation to inform also arises from the GDPR and the Law Enforcement Directive);
- limit the storage period of recordings, which may not be kept for more than one month[101] ;
- ensure the security of the processed data (for example by restricting the viewing of images to authorized persons).

97 LIL, article 44 : *"L'article 6 ne s'applique pas si l'une des conditions prévues au 2 de l'article 9 du règlement (UE) 2016/679 du 27 avril 2016 est remplie, ainsi que pour [...] 6° Les traitements nécessaires à la recherche publique au sens de l'article L. 112-1 du code de la recherche, sous réserve que des motifs d'intérêt public important les rendent nécessaires, dans les conditions prévues par le g du 2 de l'article 9 du règlement (UE) 2016/679 du 27 avril 2016, après avis motivé et publié de la Commission nationale de l'informatique et des libertés rendu selon les modalités prévues à l'article 34 de la présente loi." ("Article 6 shall not apply if one of the conditions laid down in Article 9(2) of Regulation (EU) 2016/679 of 27 April 2016 is fulfilled, as well as for [...] 6° Processing operations necessary for public research within the meaning of Article L. 112-1 of the Research Code, provided that grounds of substantial public interest make them necessary, under the conditions laid down in g of 2 of Article 9 of Regulation (EU) 2016/679 of 27 April 2016, after a reasoned and published opinion of the Commission nationale de l'informatique et des libertés issued in accordance with the procedures laid down in Article 34 of this Act".).*

98 LIL, article 32 : *"Sont autorisés par décret en Conseil d'État, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés, les traitements de données à caractère personnel mis en œuvre pour le compte de l'État, agissant dans l'exercice de ses prérogatives de puissance publique, qui portent sur des données génétiques ou sur des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes." ("The processing of personal data carried out on behalf of the State, acting in the exercise of its prerogatives as a public authority, which relates to genetic data or biometric data necessary for the authentication or verification of the identity of persons, shall be authorised by decree of the Conseil d'État, issued after a reasoned opinion has been given and published by the National Commission for Information Technology and Civil Liberties").*

99 CSI, Article L. 251-2.

100 For more information see: "Vidéoprotection: quelles sont les dispositions applicables", CNIL, 13 December 2019: https://www.cnil.fr/fr/videoprotection-quelles-sont-les-dispositions-applicables

101 CSI, Article L.252-5.

The installation of a video protection device in the public space must in principle be authorized by the prefect with territorial jurisdiction, following the opinion of the Departmental Video Protection Commission. If the systems installed are used for the processing of personal data, their installation must be authorized under the conditions laid down in the regulations applicable to the processing of personal data[102]. It therefore follows that the installation of video protection devices incorporating facial recognition technologies from the outset are subject to the provisions of the regulations on personal data processing. However, if video protection devices are installed and, as a result of this installation, facial recognition technologies are used from the recordings, it will then be necessary to comply with both standards.

NGOs denounce a system combining video protection and facial recognition in Marseille

Two NGOs, La Quadrature du Net and the Ligue des droits de l'Homme (LDH), filed an appeal with the administrative court of Marseille on 17 January 2020 to halt the deployment of facial recognition technologies based on a network of around fifty video protection cameras. The complainants criticized the City of Marseille for having implemented this system without a prior impact assessment or consultation of the French data protection authority and without establishing the absolute necessity of using such technology. However, that action was dismissed on March 11, 2020 in the absence of evidence allowing for the establishment of the contested decision.

APPROACHES ABROAD

Like France, no foreign country has so far chosen to adopt specific regulations on facial recognition technologies. Nonetheless, their use is increasing globally and within a variety of regulatory frameworks. While it is difficult to establish a clear map of the legal initiatives being undertaken abroad, some trends are discernible. Overall, the approach favoured by our European neighbours seems to be that of caution (regulation/experimentation). However, the United Kingdom stands as an exception with its relatively "open-minded" adoption of facial recognition technologies, including for security purposes in public spaces. In China, it is rather the learning-by-doing approach that is taken. Finally, in the United States, the approach is gradually moving towards regulation, or even prohibition in some states.

In Europe

The United Kingdom is the only country in Europe to use facial recognition technologies in public from "real" databases, that is, outside of tests (as was the case in the city of Nice). Across the Channel, facial recognition technologies have been deployed at several major public events, including concerts and rugby matches. This was also the case for the 2017 UEFA Champions League final in Cardiff. This particular case also led to the first arrest using a facial recognition system, of an offender wanted for domestic violence.

On 4 September 2019, a first decision was issued by the Queen's Bench Divisional Court of the High Court of Justice sitting in Cardiff. The English courts considered that the use of facial recognition technologies was in line with their laws[103]. An appeal has been launched against this decision.

102 CSI, Article L252-1.

103 High Court of Justice, Queen's Bench Divisional Court, Cardiff, Case No: CO/4085/2018, R (Bridges) v CCSWP and SSHD: https://www.judiciary.uk/wp-content/uploads/2019/09/bridges-swp-judgment-Final03-09-19-1.pdf

The ICO encourages the establishment of a binding code of practice on the use of facial recognition by the police in public places

In August 2019, a property developer installed and tested a system using facial recognition at King's Cross, a busy area of London. The system installed on the corner of one of the company's buildings was filming passers-by in the street without alerting them. The police had apparently shared "*watchlists*» with the company to carry out operations to identify persons on file. The Information Commissioner's Office (ICO), the UK equivalent of the CNIL, is currently investigating the company's use of facial recognition. As a result of this case, the ICO published a report on the use of facial recognition technologies by police in public places. Additionally, in a press release, the Information Commissioner called on the government to adopt a binding code of practice on the subject, while reminding the police that they must slow down and justify any use made of these technologies.

In Germany, the legislator has made use of the authorization provided in Article 9(2)(j) of the GDPR providing that sensitive data may be processed without consent for scientific research purposes where it is necessary for that purpose and where the interests of the controller far outweigh the interests of the data subject. On the other hand, a bill aimed at updating the current text regulating the powers of the police has been purged of its explicit references to facial recognition[104], as the Federal Data Protection Officer and the German Bar Association have expressed doubts about the bill's compatibility with the Constitution.

In the Netherlands, the legislator has also made use of the authorization provided for in Article 9(2)(j) of the GDPR on the condition that the processing is necessary for the purposes of scientific research, that the research is in the public interest, that the request for explicit consent proves impossible

104 An earlier version of the bill envisaged authorizing the federal police to use facial recognition technologies based on images collected from 135 railway stations and 14 airports.

or involves disproportionate effort, and that the execution provides for safeguards to ensure that the privacy of the data subject is not disproportionately affected.

Outside of Europe

In the United States, the Federal Trade Commission (FTC) published best practices in October of 2012 for companies wishing to develop and market facial recognition technologies[105]. Many U.S. states are making use of facial recognition technologies, sometimes for fraud control purposes (Texas[106], Washington[107] and Illinois[108] among others), sometimes for identity verification (Montana[109], Nevada[110], Connecticut[111]and North Dakota[112]). The year 2019 and the beginning of 2020 have been particularly eventful in terms of the use of facial recognition technologies in the United States:

- In March 2019, the *Commercial Facial Recognition Privacy Act of 2019* was introduced in the Senate. The Act requires private companies to obtain consent from individuals before using facial recognition technologies;
- In May 2019, San Francisco became the first U.S. city to ban its use by police and city departments. Other cities have followed suit, including Oakland and Berkeley;

105 "FTC Recommends Best Practices for Companies That Use Facial Recognition Technologies", FTC, 22 October 2012: https://www.ftc.gov/news-events/press-releases/2012/10/ftc-recommends-best-practices-companies-use-facial-recognition
106 Texas Transportation Code, Title 7, Subtitle B, Chapter 521, Subchapter A: https://statutes.capitol.texas.gov/Docs/TN/htm/TN.521.htm
107 Washington State Legislature, RCWs, Title 46, Chapter 46.20, Section 46.20.037: https://app.leg.wa.gov/RCW/default.aspx?cite=46.20.037
108 Illinois General Assembly, Illinois Compiled Statutes, Public Health (410 ILCS 705/): http://www.ilga.gov/legislation/ilcs/ilcs4.asp?DocName=041007050HArt%2E+15&ActID=3992&ChapterID=35&SeqStart=3000000&SeqEnd=6400000
109 Montana Code annotated 2019, Title 1 'General Laws And Definitions', 'Chapter 5 'Proof And Acknowledgment Of Instruments Notaries Public', Part 6. Notarial Acts, 1-5-602. 'Definitions': https://leg.mt.gov/bills/mca/title_0010/chapter_0050/part_0060/section_0020/0010-0050-0060-0020.html
110 Nevada Revised Statutes, Chapter 133 'Wills", NRS 133.085: https://www.leg.state.nv.us/NRS/NRS-133.html#NRS133Sec085
111 General Statutes of Connecticut, Volume 6, Chapter 319o, Department of Social Services, Sec. 17b-30. 'Biometric identifier system' : https://www.cga.ct.gov/current/pub/chap_319o.htm#sec_17b-30
112 North Dakota Century Code, Chapter 44-04 'Duties, Records, and Meetings': CHAPTER 44-04: https://www.legis.nd.gov/cencode/t44c04.pdf

- On October 8, 2019, California passed the *Body Camera Accountability Act* (or "AB 1215") prohibiting the use of facial recognition on body cameras worn by police officers; in the same vein, the City of San Diego, whose police had been using facial recognition technologies since 2012, decided to ban their use for at least three years, as they had not led to any arrests or prosecutions;
- In October 2019, in the state of New York, a proposal was presented requiring companies to inform users about the use of facial recognition technologies, the length of time that data is stored and its transfer to third parties;
- On November 14, 2019, a bill was introduced in the Senate, which requires federal officers to obtain judicial approval before using facial recognition technology to monitor a suspected criminal[113];
- On March 31, 2020, Washington State passed a law requiring government agencies to obtain a warrant prior to any use of facial recognition technology, except in cases of emergency[114]. According to this law, the device used must also be able to be independently tested to ensure that it does not present bias based on skin colour, gender, age and other characteristics. The law also requires, prior to any deployment by State or local authorities, the drafting of accountability reports[115] and officer training.

113 Senate of the United States, 116th Congress, 1st Session, "Bill to limit the use of facial recognition technology by Federal agencies, and for other purposes": https://www.coons.senate.gov/imo/media/doc/ALB19A70.pdf

114 "Washington State Signs Facial Recognition Curbs Into Law; Critics Want Ban", *U.S. News*, 31 March 2020: https://www.usnews.com/news/us/articles/2020-03-31/washington-state-adopts-facial-recognition-rules-critics-view-as-too-loose

115 "Washington State's regulation of facial recognition technology: first thoughts", *Global Partners Digital*, 24 April 2020: https://www.gp-digital.org/washington-states-regulation-of-facial-recognition-technology-first-thoughts/

The FBI and the U.S. Immigration and Customs Enforcement Agency involved in a controversy

In July 2019, it was revealed that the FBI and the U.S. Immigration and Customs Enforcement (ICE) had scanned the faces of millions of Americans without their consent through driver's license databases and used these images in conjunction with facial recognition technologies. However, this use was never authorized by the U.S. Congress and the citizens concerned were never informed of the use of their personal data and photographs. Nearly 390,000 facial recognition searches have reportedly been conducted by the FBI since 2011.

In China, for several years now, the governance model has been built on the basis of the massive collection and processing of citizens' personal data on social networks and through surveillance cameras. A social credit system has even been established in some regions and allows the authorities to assign scores to citizens based on their behavior. If their score is too low, individuals are punished by being deprived of their most basic rights (access to credit, movement by train, access to school). In China, facial recognition data constitutes "personal information" under Article 76 of the Cybersecurity Law[116]. However, there is no unified regulatory framework for facial recognition, but rather a multitude of sector-specific rules:

- on 21 January 2020, the Payments & Clearing Association of China published a Self-Regulation Agreement for the offline facial recognition payment industry;
- a law that came into force in December 2019 requires mobile telecommunications operators to register the biometric facial data of any new user seeking to subscribe to their services.

116 "Translation: Cybersecurity Law of the People's Republic of China (Effective 1 June 2017)", *New America*, 29 June 2018: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/

In November 2019, a first complaint was filed in the country against a company using facial recognition technologies. A law professor, who owned a pass to access a natural reserve, alleged a contractual violation against the park that changed the method of identification at the entrance.

Generally speaking, China takes a learning-by-doing approach to the legal framework of facial recognition technologies. There, their use is not limited beforehand by the legislator, but on the contrary is restricted by the technical possibilities of manufacturers. However, as part of the strengthening of the regulatory regime for the protection of personal information, the state authorities in charge of supervising the Chinese market published a new version of the standards for the protection of personal information on March 6, 2020[117]. These new standards require data controllers to inform data subjects of the rules for the collection, use and storage of data derived from facial recognition technologies and to obtain their consent for the processing of their data[118].

The analysis of the legal framework applicable to facial recognition technologies shows that the development of facial recognition technologies is relatively well regulated in the EU. The GDPR, the Law Enforcement Directive, as well as national legislations (for example the *Loi Informatique et Libertés* in France) have been established to protect our personal data, including biometric data. At the top of the hierarchy of norms, fundamental rights also exist as safeguards to protect us from the deployment of facial recognition technologies that could undermine the principles of democracy and the rule of law. In order to ensure that this framework fulfils its mission, however, it is necessary to look beyond the theoretical analysis and consider its application. A legal framework is only useful to citizens if it is effectively and (easily) applicable.

117 "China tightens protection of personal information - what you need to know about the 2020 Chinese Personal Information National Standard", *Lexology*, 23 March 2020: https://www.lexology.com/library/detail.aspx?g=5a63a595-4116-4567-bea2-f6b3380540cb

118 "China introduces stricter facial recognition standards", *South China Morning Post*, 10 March 2020: https://www.scmp.com/tech/article/3074443/china-introduces-stricter-facial-recognition-standards

THE LEGAL FRAMEWORK SUFFERS FROM DEEP WEAKNESSES IN ITS IMPLEMENTATION

A VARIED APPLICATION ACROSS MEMBER STATES

The GDPR and the Law Enforcement Directive have not fully led to the harmonization of the legal framework applicable to the processing of personal data within the European Union, in particular as regards the processing of biometric data. Certain exceptions to the principle of the prohibition of the processing of sensitive data, including biometric data, require the adoption of a national or European text for their implementation. For the time being, only a few States have decided to take the step, in particular with regard to the exception for scientific research purposes. There may therefore be significant differences in the application of the framework from one member state to another, particularly in the field of research. As mentioned above, in France, the processing of biometric data in the context of research is only possible under certain conditions and only for public research purposes. At present, there is no derogation for private research as such.

Furthermore, there are no plans at present to adopt a European text which would certainly make it possible to level out the disparities between member states and harmonize the transposing rules, for example with regard to the adoption of an experimental methodological framework. A draft white paper on artificial intelligence by the European Commission leaked in January 2020, which contained a total ban for several years on the use of facial recognition technologies in European public spaces in order to allow time to assess the impacts of these technologies and regulate them. The version of the White Paper finally published on 19 February 2020 does not mention this ban and, on the contrary, paves the way for a reflection that should be engaged at the European level[119].

119 European Commission (2020), "Artificial intelligence: a European approach based on excellence and trust", p. 22: *"In order to address possible societal concerns relating to the use of AI for such purposes in public places, and to avoid fragmentation in the internal market, the Commission will*

Moreover, there are even differences of interpretation within the same state. This is what has occurred in the United Kingdom.

In France, experiments are carried out by private and public actors, most often with the advice of the CNIL. However, the results of these experiments are not shared between the various players and the service providers are fighting a battle at a distance in an attempt to impose their technology. There is currently no reliable experimentation methodology that respects citizens' rights and freedoms. Similarly, improving the performance of facial recognition technologies requires access to increasingly large image databases. For fundamental research purposes, it may therefore be appropriate to allow European and French suppliers to access databases under conditions that respect the rights and freedoms of individuals in order to preserve their competitiveness.

Finally, not all supervisory authorities in the European Union have the same means at their disposal. Overall, their effectiveness is further limited by the small budgets allocated to them by member states. In this respect, a recent report shows that the lack of technical expertise is a major obstacle to the implementation of the GDPR in Europe[120]. The report points out that out of the 28 national authorities responsible for the application of the GDPR, only 5 count more than 10 technical specialists. Indeed, data protection authorities (DPAs) are often not in a position to defend legal actions against multinational companies, which mobilize considerable financial resources to challenge the authorities' injunctions in court. As a result, DPAs are not in a position to investigate the largest digital players. It would therefore also be useful to reflect on improving the means at their disposal, in particular to enable them to audit the conditions related to the deployment of facial recognition technologies. It is urgent to give these authorities the means to check whether or not the use of facial recognition technologies is carried out in compliance with the regulation.

launch a broad European debate on the specific circumstances, if any, which might justify such use, and on common safeguards".

120 "Europe's governments are failing the GDPR - Brave's 2020 report on the enforcement capacity of data protection authorities", *Brave*: https://brave.com/wp-content/uploads/2020/04/Brave-2020-DPA-Report.pdf

ENFORCEMENT DIFFICULTIES WHICH LEAD TO INEFFICIENCIES

DIFFICULTIES IN APPLYING FUNDAMENTAL RIGHTS

While fundamental rights and the application of the "triple test" should be mandatory, it must be noted that the "triple test" is used more by the courts in the event of litigation than by the legislature. Moreover, there is no mechanism to make it binding *a priori*.

Timid application of the "triple test" by legislators and public authorities

While the "triple test" should be imposed on legislators and public authorities, it must be acknowledged that it is used sparingly and rarely in an explicit manner. It would be useful, however, to have a systematic demonstration of it, in particular in the context of the screening assessments of draft standards or during the process of adopting administrative decisions.

In the case of the experiments with facial recognition technologies that have been conducted in France, it is highly likely that the use of the "triple test" would have been useful, if only to validate their deployment, adapt it or prohibit it.

Currently, the protection of personal data and privacy is the main concern in relation to the use of facial recognition technologies, even though their deployment is likely to infringe upon other fundamental rights. Widespread use of the "triple test" would allow for a critical assessment in terms of the compatibility of uses with all fundamental rights and freedoms.

The ex post *application of the "triple test" through jurisprudence*

With regard to case law, it generally intervenes *ex post* and, more often than not, in order to punish a use or behavior. Judges make use of the principle of proportionality and have been applying the "triple test" for several decades. However, in order for them to rule on and apply the "triple test", an appeal must first be brought to them. The problems encountered in the upholding

of fundamental rights and the application of the "triple test" are therefore highly dependent on challenges brought by the persons concerned and the referral of cases to the competent courts.

As far as fundamental rights are concerned, the main applicable texts are international and European. Appeals to an international body or to the European Court of Human Rights - even though national judges may also rule on this issue - are particularly complex and lengthy[121]. In order to reach the Court of Justice of the European Union (CJEU), an action must first be brought at the national level and a preliminary question must be referred, unless an action for failure to fulfil obligations has been brought by the European Commission against a member state. In any event, these procedures are particularly time-consuming, which creates a gap with respect to the deployment of the technologies in question, which are evolving very rapidly. The judgment will thus be given when the facial recognition technology has been or is about to be deployed:

- if the technology is already deployed, there will potentially be an infringement of fundamental rights and thus also a prejudice to the persons concerned. By definition, it will no longer be possible to go back in time for those whose rights and freedoms have been violated. This raises the question of compensation for the damage suffered and the consequences of possible sanctions against States;

- if the technology is about to be deployed, it is possible to resort to the "interim release" procedure, provided that three required conditions are met: urgency, infringement of a fundamental freedom, and demonstration that the infringement of that freedom is serious and manifestly unlawful[122].

However, this requires the persons concerned to appeal to the competent courts to ensure that their fundamental rights are respected, which implies constant and regular monitoring of the texts and projects potentially deployed by the public authorities. There are, of course, rights defending associations that are committed to this mission, but they will not necessarily have the means to act, particularly if facial recognition technologies multiply. In France, La Quadrature du Net and the Ligue des droits de l'Homme regularly lodge appeals against the deployment of facial recognition technologies. They recently succeeded in having the Marseille administrative court overturn the decision by which the regional council of Provence-Alpes-Côte d'Azur had approved the implementation of an access control system based on facial comparison and trajectory tracking in the region's high schools.

In judicial matters, in the case of an appeal against a private company deploying facial recognition technology, the procedures are also long and complex. Even when summary proceedings are possible, it usually takes several months before a decision is obtained.

Eventually, it is legitimate to ask whether it is desirable to rely solely on individuals and rights associations to ensure that our fundamental rights are respected when facial recognition technologies are deployed, given the constraints inherent in the administrative and judicial procedures.

The absence of a priori *constraints*

To date, there is no *a priori* control mechanism or obligation to carry out an impact assessment prior to the deployment of facial recognition technologies on the basis of respect for fundamental rights, apart from those imposed by the rules on personal data processing. While there is a willingness to launch several experiments and to supervise them, there has not yet been any question of implementing this prior analysis with regard to fundamental rights. Yet, many voices call for an in-depth reflection on the subject of facial recognition technologies, as they have the potential to impact the very foundation of democracies. This is the case at the European level through the EU Fundamental Rights Agency (FRA) and the European Data Protection Supervisor, and also at the national level through the CNIL and through initiatives led by members of parliament.

With regard to the rules on the processing of personal data, it should be noted that the system of prior authorization has almost completely disappeared and that those involved in the processing of personal data are now responsible. Each controller must therefore carry out a risk assessment and,

121 See the diagram "*Le cheminement d'une enquête*" ("The course of an investigation") produced by the European Court of Human Rights: https://www.echr.coe.int/Documents/Case_processing_FRA.pdf

122 Code of Administrative Justice, Article L521-2.

in particular, carry out their own data protection impact assessment (DPIA). Nonetheless, the question arises of the systematic submission of DPIAs to the supervisory authorities, for example to the CNIL in France.

The European Commission, in its White Paper on Artificial Intelligence, states that *"it is vital that European AI is grounded in our values and fundamental rights such as human dignity and privacy protection*" and contemplates various certification and labeling mechanisms allowing for *a priori* review[123].

THE QUESTION OF LIABILITY

In addition to the difficulties in enforcing fundamental rights, the issue of liability is another weakness inherent in the legal framework around facial recognition technologies. This thorny problem arises differently not only from one country to another, but also according to the system of reference under consideration (protection of personal data, privacy, etc.).

Under the rules on the processing of personal data, it is first of all the controller - i.e. the person who defines the means and purpose of the processing - who is responsible vis-à-vis individuals, although the data processors may also be held liable since the entry into force of the GDPR.

Under tort law, the implementation of liability (contractual or tortious) is subject to the fulfilment of three cumulative conditions, namely fault, harm and a causal link between the two:

- Contractual liability refers to the obligation to remedy any damage resulting from a defect in the performance of a contract (non-performance, poor performance or late performance). For example, if facial recognition technologies cause direct damage to the customer-user, the supplier of these technologies could be liable to remedy the damage;
- Tortious liability refers to the obligation to compensate for harm caused to others outside of any contractual relationship. The question of the liability of suppliers of facial recognition technologies vis-à-vis third parties arises in terms substantially similar to that of artificial intelligence. In French law, the "*responsabilité du fait des choses*" is essentially based on the control of the object in question at the time of the occurrence of the harmful event, which is not necessarily adapted to artificial intelligence. The same is true with regard to product safety regulations - which impose liability on the producer of the product placed on the market - in particular when artificial intelligence is incorporated after the product has been placed on the market by a party other than the producer.

In any case, the issue of liability for facial recognition technologies must be addressed for all actors along the chain of liability, whether they are the designers of the algorithm, the solution providers, the private and public actors deploying these technologies, or the users.

The responsibility of providers is most often questioned, but the responsibility of users (operators) is perhaps not questioned enough. Facial recognition technologies provide a percentage chance that template A will match template B and, based on this result, an individual then decides whether or not intervention is necessary. It is therefore important that this individual have sufficient knowledge to make a decision, but also and above all that he or she approaches the person concerned bearing in mind that this is only a potential match and not necessarily a proven one (see this report's section on "Probabilistic technologies prone to human deficiencies").

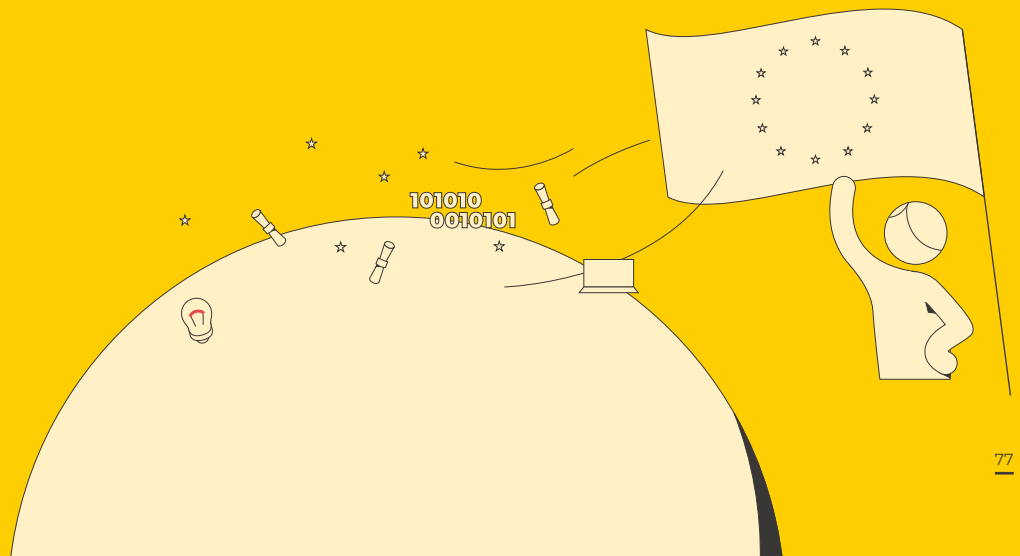
Finally, the issue of criminal liability must also be considered, which is likely to arise in particular for client-users, for example, in relation to the criminal sanctions attached to non-compliance regarding the regulations on personal data processing[124].

123 European Commission (2020), "Artificial Intelligence: A European approach based on excellence and trust", p. 2.

124 Criminal Code, Articles 226-16 and following.

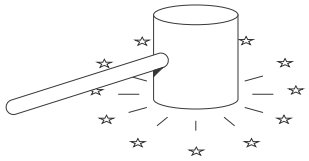
Ultimately, it must be admitted that, although the legal framework surrounding the deployment of facial recognition technologies is well provided, it suffers from serious weaknesses in its implementation. In particular, it is complex to ensure the conformity of these technologies with our fundamental rights in the absence of *a priori* scrutiny. As for the analyses carried out *ex post* by courts, these require that the matter be referred to the judge, and that a considerable investment be made by the applicant, particularly in terms of time and skills. Not everyone has the means required for this. When it comes to the protection of our personal data, and therefore of our biometric data, the lack of harmonization at the European level and the lack of resources allocated to supervisory authorities presents an issue. If our aim is to ensure that facial recognition technologies are deployed in accordance with European values, that is to say in compliance with the principles of the rule of law and democracy, then we cannot be satisfied with this current situation. At a time when more and more facial recognition technologies are being deployed, there is an urgent need for the European Union to address these issues and for member states to agree on a robust system to guarantee our rights.

PART 3
TOWARDS A EUROPEAN STANDARDIZATION SYSTEM GUARANTEEING FUNDAMENTAL RIGHTS AND FREEDOMS



The processing of contactless biometric data gives facial recognition devices a highly sensitive character that requires increased vigilance on the part of society. Leaving the door open to mass surveillance is not an option and the boundaries between the various applications of these technologies are often porous. How, therefore, can we protect ourselves from the threat to our fundamental rights and freedoms? Several pathways have emerged in the public debate over the last few months, ranging from a total ban on facial recognition technologies to improving the existing framework through the development of complementary regulations.

As regards their regulation, facial recognition technologies are currently well regulated legally within the European Union. However, what the legal analysis of this framework reveals is a profound lack of efficiency in its application, in particular with regard to respect for fundamental rights. There is a crucial area for improvement here, the aim of which must be to compel all actors in the ecosystem of facial recognition technologies to better apply the existing framework as early as in the experimentation and marketing phases. The evolving nature of these technologies must also be taken into account, in order to guarantee the robustness of a protective framework over time and prevent it from quickly becoming obsolete.



Moreover, there are strong geopolitical issues at stake in the deployment of facial recognition technologies, ranging from competition in the international market, to the defense of European sovereignty. This debate offers a unique opportunity for Europe to impose its own rules in order not only to increase its competitivity compared with the United States and China, but also to build a strong European path, one that reflects our values.

The European standardization approach therefore stands out as the best way forward. Developing our own standards would give us a chance to put respect for fundamental rights at the heart of the deployment of facial recognition technologies. Such an initiative at the European level would also encourage the harmonization and efficient application of the existing legal framework, while guaranteeing the technological independence of the European Union. Indeed, in the domain of facial recognition, it is high time for the EU to free itself from the US's grip on the international standardization market.

THE NIST'S DOMINANCE OVER INTERNATIONAL STANDARDS

THE REASONS FOR THIS PREDOMINANCE: AN INTERNATIONALLY RECOGNIZED AUTHORITY WITHOUT A EUROPEAN EQUIVALENT

With regard to biometrics, the National Institute for Standards and Technology (NIST) became the international reference centre for standardization in the 2000s. Together with industry, this agency of the U.S. Department of Commerce regularly conducts evaluations of algorithms and develops norms and standards that are then exported internationally. Because of this close collaboration with industry and given the bridges it has built with the academic world, the NIST is recognized as the most competent body in this domain. In fact, it is frequently solicited by the American government to carry out missions to evaluate the performance of algorithms, including in the area of facial recognition. Thus, great legitimacy is attributed to algorithms that are well placed in the rankings established by the NIST, and compliance with the norms and standards developed by this American agency has become an absolute priority for many producers (not only American, but also European, Russian and Chinese[125]) of facial recognition devices. The results of the famous Facial Recognition Vendor Test (FRVT) are regularly cited by

125 "Technology: how the US, EU and China compete to set industry standards", *Financial Times*, 24 July 2019: https://www.ft.com/content/0c91b884-92bb-11e9-aea1-2b1d33ac3271

technology providers as a measure of their credibility and by policy makers as a guarantee of their quality to justify usage[126].

With the diffusion in Europe of technologies based on algorithms evaluated by the NIST, the U.S. agency's testing criteria have gradually become the reference at the EU level. As a result, the evaluation criteria established by the NIST are now often put forward in European calls for tender[127]. Moreover, the European companies, including French companies, which have established themselves as leaders in the international market for facial recognition technologies are those which have accepted the American standards as their measuring stick. If these firms have been able to access the international market and gradually gain market shares, it is by complying with the NIST's standards.

This predominance is also made possible by the absence of a European equivalent to the NIST. The European Committee for Standardization (CEN), which brings together the European national standardization bodies (for example AFNOR for France[128]), has less influence in the development of supranational standards. This difference in impact between the NIST and the CEN is linked to several factors. On the one hand, the CEN is not a governmental agency. It relies on contributions from its members and, to a lesser extent, from the European Commission, for its functioning. It therefore has a relatively limited budget. On the other hand, when it comes to evaluation exercises, the U.S. agency has access to the U.S. government's vast biometric databases (provided in particular by the FBI, the State Department and the Department of Homeland Security). Over time, the NIST has built up testing bases containing millions of biometric data. In Europe, where it is difficult to collect this kind of data, such scale effects are impossible for the CEN. Last, the NIST is also working with international standards committees to develop common standards, which further strengthens its grip on the international standardization market. The NIST's financial resources and high level of expertise enable it to mobilize large delegations within these bodies, and to win the support of smaller delegations with less expertise and more limited budgets. In particular, the U.S. agency collaborates with the ISO-IEC Joint Technical Committee 1 and, more specifically, with its specialized subcommittee 37 dedicated to biometrics (see the "ISO-IEC SC-37" box).

126 "How the US plans to crack down on Chinese facial recognition tech used to 'strengthen authoritarian governments' ", *This Week in Asia*, 18 June 2019: https://www.scmp.com/week-asia/geopolitics/article/3014868/how-us-plans-crack-down-chinese-facial-recognition-tech-used

127 During the hearings conducted for this report, one industry member pointed out, for example, that questions such as: "*Is your system referenced in the NIST's FRVT?"* are found in European tenders.

128 For a complete list of CEN members, see: https://standards.cen.eu/dyn/www/f?p=204:5:0::::FSP_ORG_ID,FSP_LANG_ID:,34&cs=1177845D46C9904580CCC631EC8FE906F

The SC-37 of ISO/IEC[129]

In addition to the CEN, some European national standards bodies also meet in the framework of Joint Technical Committee 1 of the ISO-IEC international standardization body dedicated to information technology, and more specifically in the SC-37, the subcommittee dedicated to biometrics. This subcommittee is organized around six working groups, including one on "*cross jurisdictional and societal aspects of biometrics*"[130]. Each country represented within the SC-37 delegates a team through its sole ISO member (ANSI for the United States, AFNOR for France, Deutsches Institut für Normung for Germany, the British Standards Institution for the United Kingdom, etc.)[131]. These teams participate in the technical discussions of the subcommittee through written contributions. The statutes of the ISO/IEC committee provide for equal representation among countries (that is, without deciding vote casting in the decision-making process and therefore with representativeness regardless of the size of the delegation). However, the size of the delegations is not irrelevant in the decision-making mechanism. Indeed, the details of technical discussions often lead to arbitration, so that within the SC-37, the practice is to make decisions on the basis of the majority of the votes of the delegations present at the meeting. In the absence of a strong point of view

129 International Standardization Organisation (ISO)/International Electronical Commission (IEC).

130 For more information on SC-37, see: https://www.iso.org/committee/313770.html

131 For the complete list of SC-37 members, see: https://www.iso.org/committee/313770.html?view=participation

(due to the narrow scope of competence), small delegations are inclined to adopt a mimetic approach and to base their votes on personal confidence in certain delegates or delegations, or even on the surrounding political context.

The financial aspect is not neutral either in the operation of these international committees which, in order to develop a standard, rely on three to four annual meetings, sometimes spread over several years. Only large companies investing in biometrics, institutions of a certain size (the NIST, the Fraunhofer Institute) and governments significantly involved, mobilize delegates in their representation at the SC-37. The U.S. delegation is always very large. In addition to the representatives of various federal departments, it includes most of the American biometric manufacturers, who see this as an opportunity to promote their know-how in the construction of biometric standards.

Since its inception in 2002, the SC-37 has developed no less than 130 international standards for biometrics. While most of these standards are not in use (for example, the biometric sensor API[132] standard has never been as successful as hoped), some of them are effective and widely applied worldwide. This is the case of the ISO/IEC 19794-2, 19794-4, 19794-5 and 19794-6 standards on biometric data exchange formats, which are almost systematically included in calls for tenders involving biometrics. Standard 19794-5, for example, defines the criteria to be met for the photos used on our ID cards[133].

This is therefore a crucial issue for the European Union, which must mobilize the means to invest fully in these bodies. In order to lend greater force to this action, the European strategy must be collective, rather than the result of isolated players from different member states.

132 *Application programming interfaces.*
133 See: https://www.diplomatie.gouv.fr/IMG/pdf/depliant_norme_photo-2.pdf

THIS PREDOMINANCE MUST BE QUESTIONED

Behind this predominance lie two challenges for Europe: to maintain a certain technological independence from the United States, and to adopt values that are not necessarily ours. In the global digital ecosystem, the predominance of the United States and China, and Europe's relative technological lag, raises the question of the control of data. This issue is particularly acute in the context of facial recognition technologies, which are based on the processing of biometric data, which are among the most sensitive data.

Furthermore, the criteria established and used by the NIST, notably in the Face Recognition Vendor Test (FRVT), widely considered the standard measure for determining the reliability of facial recognition software[134], are exclusively technical. As explained in the report "Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects"[135] published in December 2019, the performance of systems subject to the FRVT is mainly analyzed according to one criterion: accuracy[136]. This accuracy is reported by the American agency through an error rate, or the number of Type I or "false positive" errors (when an individual is incorrectly associated with another person) and Type II or "false negative" errors (when an individual is not associated with him or herself) committed by the algorithms in question. Algorithm execution time and "demographic differentials" (variations in precision based on demographic group[137]) are also taken into account. At the end of the test, the algorithms are ranked by the NIST, from the most to the least performant[138], based on these criteria.

However, when it comes to facial recognition technologies, the reliability of a system cannot simply be measured by its technical performance. If we consider the protection of personal data and respect for fundamental rights as essential attributes, then reliable facial recognition technology is not only a

134 "How the US plans to crack down on Chinese facial recognition tech used to 'strengthen authoritarian governments' ", *This Week in Asia*, 18 June 2019: https://www.scmp.com/week-asia/geopolitics/article/3014868/how-us-plans-crack-down-chinese-facial-recognition-tech-used
135 National Institute of Standardization and Technology (2019), "Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects", U.S. Department of Commerce, 82 pp.
136 *Ibid.*, p. 20.
137 The criteria used to assess these "demographic differentials" are the age, sex and place of birth (referring to ethnic origin) of individuals.
138 For an example of a NIST ranking, see: https://pages.nist.gov/frvt/html/frvt11.html

high-performance technology. It is a technology we can trust because it will not lead to the usurpation of our identity, the uncontrolled sharing of our biometric data, the intrusion into our privacy without prior consent, or the massive remote surveillance of our actions. Despite recent initiatives by the U.S. Senate to prohibit companies that do not respect human rights from submitting their algorithms to the FRVT[139], there is still a long way to go. In any case, taking these criteria into account means establishing intrinsically European specifications that correspond to our vision of the digital society: a society that is inclusive and respectful of fundamental rights and freedoms.

As was the case in the field of personal data protection, this situation offers an unprecedented opportunity for Europe to break free from American dominance by proposing and promoting its own standards, in order to effectively protect the rights of its citizens.

MAKING EUROPEAN STANDARDS A LEVER FOR PROTECTING CITIZENS

As stated in its preamble, the purpose of the Charter of Fundamental Rights of the European Union is "*to strengthen the protection of fundamental rights in the light of changes in society, social progress and scientific and technological developments*". If the European Union wants to ensure that its values and principles are effectively protected and taken into account in the deployment of facial recognition technologies, it must invest more heavily in the global standardization race. In order to assert itself, the European Union can count on its soft power (see the "The Brussels effect" box), as has been the case with the adoption of the GDPR. However, this framework suffers from variations in its application between countries. This is why bringing together the initiatives of the different member states around this standardization must be a priority. This is all the more important since, as highlighted by the European Commission in its White Paper on Artificial Intelligence, some EU members are already embarking on unilateral initiatives to regulate AI applications[140].

The 'Brussels effect'

In the global race for standardization, the European Union stands out from the two other major leaders in the digital market, which are the United States and China. While China has adopted an aggressive strategy to push the spread of its standards worldwide, and the Trump administration has engaged in a genuine economic war with China, the European Union is relying on its soft power and more particularly on the 'Brussels effect' to impose its values[141]. This term, coined by a journalist at the Financial Times, refers to the fact that certain rules laid down by the EU (particularly in the automotive, chemical and food industries) have gradually been adopted worldwide. The GDPR is the most recent example in the digital domain: many countries around the world are implementing laws on the regulation of personal data that are strongly inspired by this EU regulation. This is also the case of California, which frequently takes the lead in regulation in the United States[142]. It remains to be seen whether the EU will be able to use this 'Brussels effect' to make its mark in the global market for the standardization of facial recognition technologies.

139 "Senators introduce bill to regulate facial recognition technology", *The Hill*, 14 March 2019: https://thehill.com/policy/technology/434166-bipartisan-senators-introduce-bill-to-regulate-facial-recognition

140 European Commission (2020), "Artificial Intelligence: A European approach based on excellence and trust", p. 10: "*The German Data Ethics Commission has called for a five-level risk-based system of regulation that would go from no regulation for the most innocuous AI systems to a complete ban for the most dangerous ones. Denmark has just launched the prototype of a Data Ethics Seal. Malta has introduced a voluntary certification system for AI. If the EU fails to provide an EU-wide approach, there is a real risk of fragmentation in the internal market, which would undermine the objectives of trust, legal certainty and market uptake*".

141 "Technology: how the US, EU and China compete to set industry standards", *Financial Times*, 24 July 2019: https://www.ft.com/content/0c91b884-92bb-11e9-aea1-2b1d33ac3271

142 *Ibid.*

ACCOUNTING FOR BOTH TECHNICAL AND LEGAL ASPECTS

Whereas the American standards currently prevailing on the market are based exclusively on characteristics relating to the technical performance of algorithms, Europe must distinguish itself by introducing a legal dimension into its standards. Taking these aspects into account is essential if we are to ensure that the development of facial recognition technologies is respectful of European values. Moreover, the current standards, which are based on simple rankings, can be perfected even from an algorithmic performance perspective. In the process of developing European standards for facial recognition technologies, it is therefore essential not to neglect these aspects.

Whatever the ultimate use of facial recognition technologies, it is important to ensure that the algorithms are fair, that is that they perform the tasks for which they were designed as effectively as possible.

In this regard, although the NIST takes into account a certain number of criteria in its FRVT (error rates, execution time, demographic differentials) in order to evaluate the performance of algorithms in relation to each other and the performance of a given algorithm over time, the U.S. agency does not issue technical certifications. The NIST evaluations are not intended to mean "this system conforms to our standards, while this one does not". Instead, algorithms are ranked from most to least efficient. So how can we determine which systems have an "acceptable" level of performance for large-scale deployment? Should the top 100 be considered? The top 500? The European standards must therefore take the technical criteria used by the NIST as a basis, but also introduce evolving thresholds. For each criterion analysed, whether it be the error rate, execution time or demographic differentials, defining a threshold below which the system is deemed to be non-compliant would result in more precise standards and would allow to set up a real certification mechanism. Algorithms classified below the threshold (for example, those whose results in terms of managing discriminatory biases are deemed too low) would not receive certification. In order to take into account technological developments over time, such thresholds need to be adaptable.

While these technical aspects should form the first pillar of European standards for facial recognition technologies, the second pillar should deal with legal aspects. For the time being, these are completely absent from the standards established by the NIST.

In April 2019, the High-Level Expert Group on Artificial Intelligence, set up by the European Commission, published its "Ethical Guidelines for Trustworthy AI"[143]. In the document, the experts identify seven essential requirements for AI, namely: (1) human action and human control; (2) technical robustness and security; (3) privacy and data governance; (4) transparency; (5) diversity, non-discrimination and fairness; (6) societal and environmental well-being; and (7) accountability[144]. More recently, in its White Paper on Artificial Intelligence, the European Commission has taken up a number of these requirements and clarified them for so-called "high-risk" AI applications. Among the Commission's recommendations is the need to establish specific requirements for remote biometric identification, including compliance with the Charter of Fundamental Rights[145].

Although what exactly constitutes a "high-risk" artificial intelligence application remains to be defined, the European Commission refers in its White

143 High Level Group of Independent Experts on Artificial Intelligence set up by the European Commission in June 2018 (2020), "Ethical Guidelines for Trustworthy AI": https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top

144 *Ibid.*, p. 3.

145 European Commission (2020), "Artificial Intelligence: A European approach based on excellence and trust", Communication, COM(2020) 65 final, p. 21.: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

Paper to the example of the deployment of facial recognition technologies in public places[146]. However, in an approach based on standardization, there is no need to distinguish between uses. All use cases, regardless of their degree of sensitivity, should respect the above-mentioned criteria. In other words, any deployment (including experimentations) of a facial recognition system must pass a test with regard to fundamental rights. As such, each deployment must first:

- be provided for by law;
- genuinely meet objectives of general interest recognized by the European Union, or the need to protect the rights and freedoms of others;
- respect the essence of rights and freedoms, that is, the inalienable core of the right concerned;
- be necessary (principle of necessity);
- respect the principle of proportionality (which requires passing the "triple test")[147].

In fine, only technologies that bring together all these dimensions would be considered respectful of our fundamental rights and could be implemented.

146 *Ibid.*, p. 25.
147 According to the "triple test", a measure restricting fundamental rights must be appropriate, necessary and proportionate.

TABLE 2 - ESSENTIAL CRITERIA FOR EUROPEAN STANDARDS APPLICABLE TO FACIAL RECOGNITION TECHNOLOGIES[148]

Technical criteria	For all uses: criteria established by the NIST (error rate, speed of execution, demographic differentials) enriched with evolving performance thresholds
Legal criteria	For all uses: respect for the EU Charter of Fundamental Rights Depending on the practice: compliance with the GDPR or the Law Enforcement Directive and other norms specific to the member states (for example, in France, the *Loi Informatique et Libertés*)

ENSURING THE ADOPTION OF EUROPEAN STANDARDS BY ENFORCING COMPLIANCE IN PUBLIC PROCUREMENT CONTRACTS

In any event, the definition of standards to accompany the deployment of facial recognition technologies on the European continent cannot be an end in itself. These standards must effectively fulfill their mission: to guarantee harmonization and efficiency in the application of the existing legal framework. In the practical implementation of the standardization system, thought must therefore be given to how to encourage compliance with and dissemination of standards. As standards are voluntary, this must be part of a performative approach.

148 It should be noted that we do not mention among the essential criteria certain major principles inherent to all technologies based on artificial intelligence or to digital technology in general. However, it goes without saying that, as far as possible, the facial recognition technologies used on the continent must also integrate the principle of "green technology" into their operation, in accordance with the European Green Deal presented by the European Commission in December 2019.

The first step in this process would be to impose compliance with standards in the context of European, national and local public procurements, including for experimentations. In concrete terms, this means awarding public contracts only to organizations that comply with the standards in question for all facial recognition technologies, regardless of the degree of risk. This obligation would make it possible to guard against initiatives that are currently emerging in territories without sufficient supervision and without any attempt to find alternatives. To this end, calls for tenders should contain criteria for assessing the proposed solutions against European standards. Failure to comply with the standards would be detrimental to the operators present on the market (and those wishing to enter it), and the latter would be encouraged to comply with it either by taking them into account during the system development phase or by bringing existing systems into conformity.

This "levelling up" should have a performative effect and enable European standards to become the benchmark for the deployment of facial recognition technologies within the EU, whether their manufacturers are based there or not, for both public and private contracts. Furthermore, in addition to their dissemination, the imposition of standards in the context of public procurement would provide an effective framework for public surveillance. The final stage in the adoption of European standards for facial recognition would be their international dissemination through the famous 'Brussels effect'.

However, all of this requires the ability to monitor compliance with the standards at the EU level, which means that European bodies must be able both to set and audit these standards.

A EUROPEAN GOVERNANCE DEDICATED TO THE STANDARDIZATION OF FACIAL RECOGNITION TECHNOLOGIES

While the current framework for facial recognition technologies is characterized by a disparate application at the EU level, the development of a common reference framework for all member states inevitably requires that all relevant actors pool their knowledge through a multi-stakeholder body responsible for these standards.

GATHERING EXPERTISE WITHIN A MULTI-STAKEHOLDER BODY

Although it should be revisited, the ecosystem of actors likely to be involved in the control of European standards relating to the deployment of facial recognition technologies does not need to be completely built from scratch. For the time being, this ecosystem is essentially made up of a network of national data protection authorities and national standardization agencies that we find at the European level within various authorities. The body responsible for European standards in the field of facial recognition should rely on these organizations to draw up a common frame of reference for all member states[149].

In particular, such a body could rely on the European Committee for Standardization (CEN), which brings together the national standardization organizations of the member states and whose primary mission is the production of European safety and quality standards. This body has been working on facial recognition technologies for several years, but this work merits an update. In its 2016 annual report, the Committee announced that it had ap-

149 This principle, according to which priority should be given to existing bodies, was also reiterated on 12 May in the framework of the European Commission's JURI Committee by the shadow rapporteurs of the PPE, Renew, ECR and ID Groups. The latter were opposed to the idea of creating a *"European agency for AI"* defended by MEP Iban Garcia del Blanco (S&D) and proposed instead to rely on existing authorities. See: https://multimedia.europarl.europa.eu/en/juri-committee-meeting_20200512-0900-COMMITTEE-JURI_vd

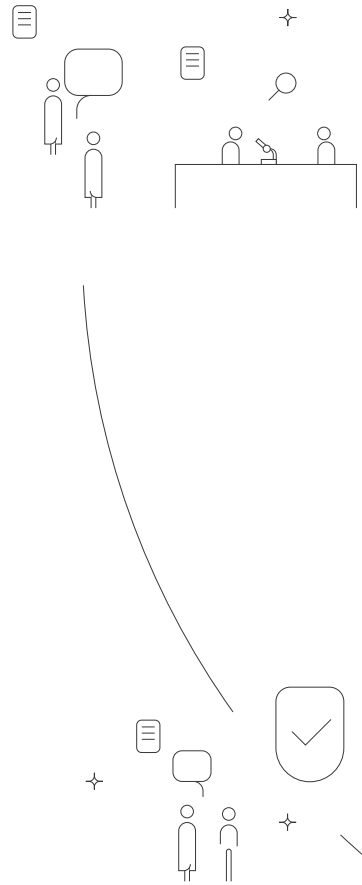
proved a work program aimed at reaching "*an agreement on the upcoming drafting of a European Standard on 'Privacy protection by design and by default' and on sector-specific guidelines for video surveillance (CCTV) and biometric measures for access control including face recognition*"[150]. While the area of privacy protection by design and by default has since been taken over by the European Data Protection Board (EDPB)[151], the area of biometrics seems to have been somewhat neglected[152].

In addition to the national standardization organizations, it is crucial to involve representatives of the EDPB[153], i.e. national data protection authorities (the CNIL in France and its European counterparts)[154], in this body. The protection of biometric data - highly sensitive data - must indeed be at the heart of the European standardization system.

As the development of European standards must also account for the respect for fundamental rights, it is essential that the representatives of the CEN and the EDPB work closely with the experts of the EU Fundamental Rights Agency within this body. The Agency provides independent expert advice and analysis on fundamental rights to EU institutions and member states. It is the body best placed to contribute to the mainstreaming of the "triple test". In addition, the EU Agency for Fundamental Rights has a particularly close working relationship with the national authorities responsible for defending rights, who must be involved in the development of European standards for facial recognition technologies. In France, the *Défenseur des droits* notably protects the rights of users of public services and the rights of the child, and actively fights against discrimination.

This pooling of knowledge and skills with a view to drawing up European standards and making them understandable both for the industry and supervisory authorities could require the creation of working groups, each dedicated to a specific topic (e.g. technical aspects, data protection, fundamental rights, cross-cutting rights, transparency, etc.).

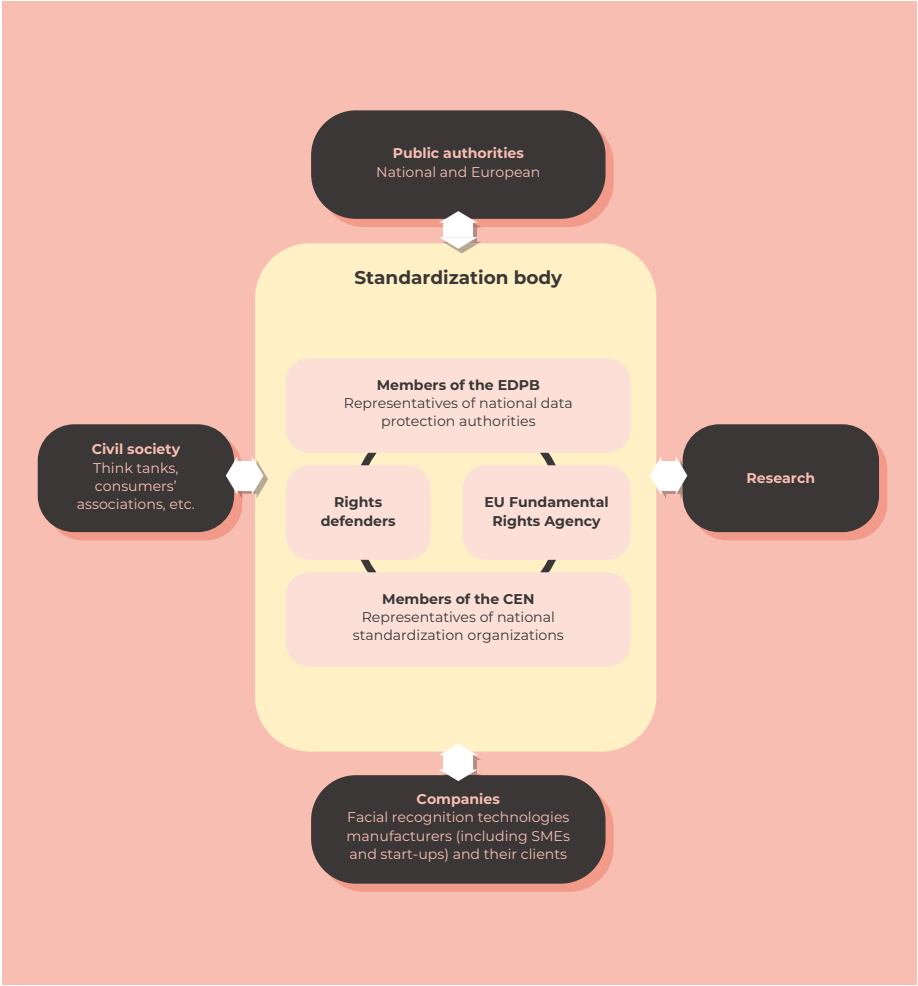
For this system to be truly comprehensive and democratic, the standardization body's discussions should also include consultation with civil society (think tanks[155], consumer associations, advocacy groups), the research community, businesses and public authorities, on the implementation of standards and their further development (see Figure 3 "The structure of the European standardization body for facial recognition technologies"). In order to avoid redundancy, this work should also be carried out hand in hand with the relevant Directorates-General of the European Commission[156].



150 European Committee for standardization (2017), Annual Report 2016, p. 9: https://www.cen.eu/news/brochures/brochures/Annual_Report_2016_Tome_1_accesibility.pdf
151 European Data Protection Board (2019), "2018 Annual Report: Cooperation & Transparency", p. 25: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_annual_report_2018_-_digital_final_1507_en.pdf
152 There is no mention of this in the 2017 and 2018 NEC activity reports.
153 Not to be confused with the European Data Protection Supervisor (EDPS).
154 For a complete list of EDPB members, see: https://edpb.europa.eu/about-edpb/board/members_en

155 For example, the *Biometric Institute*, which is doing a lot of work on the subject.
156 For example, DG Justice is currently working on the development of a standard for fingerprint recognition.

FIGURE 3 - THE STRUCTURE OF THE EUROPEAN STANDARDIZATION BODY FOR FACIAL RECOGNITION TECHNOLOGIES



Not only does monitoring adherence to standards at the EU level require a body dedicated to their elaboration, but it also requires that these standards be auditable.

PUTTING AUDITABILITY AT THE HEART OF THE STANDARDIZATION SYSTEM

Auditability is the foundation of any standardization system. If our standards are not auditable, then we have no way of monitoring their compliance. Establishing these standards should make it possible to draw up a certification reference framework[157] common to all the member states of the EU. This certification reference frame for European facial recognition technologies must include the list of requirements to be verified, translating in a clear and affordable manner the standards established by consensus within the standardization body.

Once the reference framework has been established, that is once the legal principles (in particular the "triple test") and the technical aspects have been translated into practical requirements, it becomes possible for a European inspection body to audit a device with a view to its certification. This is where the idea of imposing standards in public procurement takes on its full meaning. If a manufacturer of facial recognition technology hopes that their device will be selected in a public tender, then they will have every interest in having it certified by a competent independent body. Without such certification, their application will not be successful[158]. This mechanism allows both the company and the authority using a facial recognition technology to prove that it meets the established standards, and to assure citizens that the device to which they are subject is trustworthy (not only from a technical point of view, but also from an ethical point of view).

It should be noted here that certification is granted for a limited period of time, during which the certifying body carries out monitoring. Furthermore, since facial recognition technologies are devices that are constantly evolving

157 That is to say, a *"technical document defining the characteristics that an industrial product or service must have and the arrangements for checking its conformity with those characteristics*". See Ministry of Economy, Finance and Industry (2004): "La certification en 7 questions des produits industriels et des services", p.4.: https://evaluation.cstb.fr/doc/certification/certification-en-7-questions.pdf

158 It should be noted that care should be taken to ensure that the standardization system does not become a barrier to new entrants. All companies, from very small businesses to multinationals, must be able to develop technologies that comply with the standards. Hence the need to consult also the smaller players in the implementation and further development of the standards (see diagram "The structure of the European standardization body for facial recognition technologies").

with innovation, perhaps a notification mechanism should be considered to alert the certifying body about changes over time in a technology that it has certified. This would involve the manufacturer of the technology notifying the body of any significant changes to the device in question, with a view to reassessing the certification. This monitoring should focus on significant changes to the functionality of the product that may significantly affect its performance in testing or the nature of the safety information to be provided. Updates such as security patches or simple enhancements should not trigger a new risk assessment after a technology has been placed on the market.

However, this compliance check requires the ability to compare the algorithms on which facial recognition technologies are based with large, centralized image databases, which is particularly difficult in the EU at present. Although regulation allows this under certain conditions, several principles of the GDPR hinder the creation of large centralized databases. To this end, it is crucial for the European Union to develop a doctrine to encourage innovation in artificial intelligence, while at the same time preserving the core principles of the GDPR.

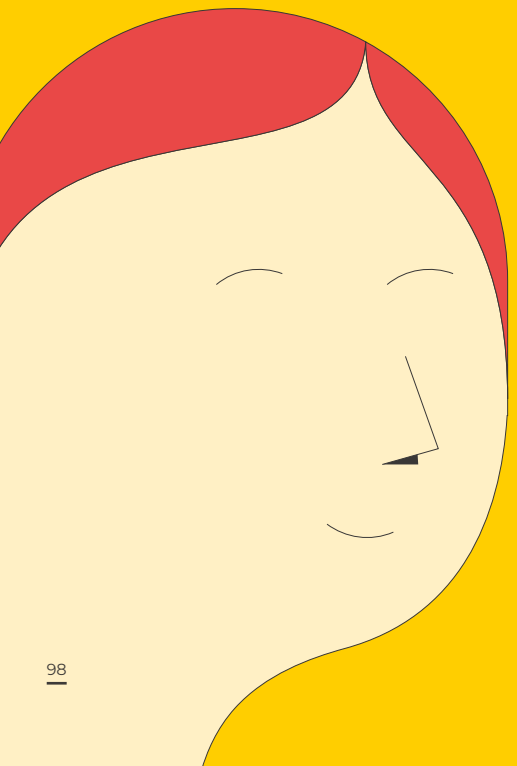
Beyond the implementation of this certification mechanism based on third-party auditing (independent certifying offices/bodies), having a reference system at the European level would also allow self-auditing of companies developing and/or using facial recognition technologies. The latter must be able to appropriate the reference system in order to carry out *a priori* impact assessments. The possibility of this self-assessment in relation to the standard is all the more necessary since the almost complete disappearance of the system of prior authorization with the entry into force of the GDPR. While it is not currently the case, we could imagine requiring the transmission of the results of these impact assessments to the national supervisory authorities (to the CNIL, for example), so that they can issue opinions. However, self-auditability is not intended to replace third party certification. It is a voluntary approach on the part of the manufacturer enabling them to take into account the requirements of the European standards from the design stage. Since the certification process has a cost, it is essential for a manufacturer to make sure that their certification application has the best possible chance of being accepted.

Finally, in addition to third-party certifiers and technology providers, the authorities responsible for monitoring compliance with the standards must also be able to appropriate the standard. This is indispensable not only for the purpose of generalizing the use of the “triple test” (legal aspect), but also to increase the effectiveness of the supervision of technical aspects. Consequently, regulators must step up their efforts. Carrying out impact assessments on complex technologies is an extremely time-consuming task which requires extensive resources, not only budgetary but also (and just as importantly) human resources (highly qualified staff). As things stand at present, these resources are far from assured[159]. There is an urgent need for member states to show real political will and provide their supervisory authorities with the resources they need. In addition to financial resources, this also requires a significant training effort.

> While the establishment of this European standardization system emerges as the option most likely to guarantee a deployment of facial recognition technologies that respects European values, achieving this project will not be easy. Increased cooperation between national authorities within a European body, as well as investment (financial and human resources) by member states appear to be the *sine qua non* conditions for the success of such an undertaking. Failure in this mission would contribute to the erosion of European digital sovereignty and to the potential undermining of the democratic guarantees of the rule of law. It is thus not an option.

159 *Brave, op. cit.*

CONCLUSION
THE EU'S OPPORTUNITY TO PLACE HUMANS AT THE HEART OF THE SYSTEM



In light of the current predominance of U.S. standardization, and as the deployment of facial recognition devices accelerates internationally, it is crucial that the European Union build a system that guarantees its values. It is estimated that by 2024, the market for facial recognition technologies will generate revenues of $7 billion (more than double the $3.2 billion recorded for 2019)[160].

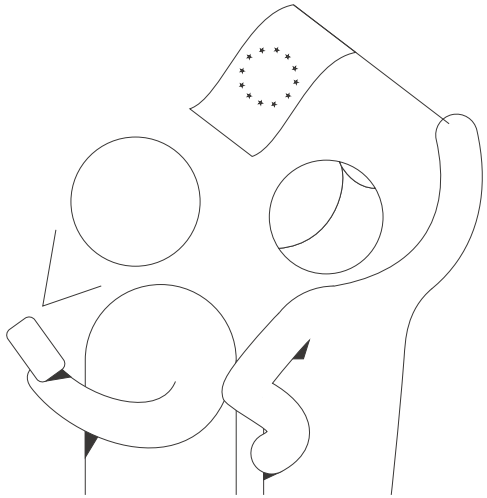
Beyond the guarantee of citizens' rights, there is also, in the implementation of European standards applicable to facial recognition technologies, an important issue of digital sovereignty.

However, the European strategy cannot be based solely on the implementation of auditable European standards. In addition to establishing a standardization system that guarantees a trusted technology, the essential issue is to give control to humans. Whether they are public or private players, users of facial recognition technologies play a major role in the deployment of these technologies across territories. As such, the highly sensitive and intrusive nature of these technologies must always prompt the question of an alternative. It is also necessary to ensure, including in the private sector, that individuals are enabled to interact with these technologies in the best possible way. In this respect, it is the responsibility of users to explicitly inform citizens about the deployment of a facial recognition device, so that they can make a conscious decision

160 "Facial Recognition Market by Component (Software Tools (2D Recognition, 3D Recognition, and Facial Analytics) and Services), Application Area (Emotion Recognition, Access Control, and Law Enforcement), Vertical, and Region - Global Forecast to 2024", *Markets & Markets*, June 2019: https://www.marketsandmarkets.com/PressReleases/facial-recognition.asp

as to whether or not to subject their face to biometric processing. An awareness campaign at the European level should also be deployed, with the aim of informing citizens and enabling them to exercise their rights. It is essential that each individual who is subjected (voluntarily or involuntarily) to a facial recognition device understand their rights and remedies, where their data are sent, for what purposes, by whom they are processed, for how long, what risks they run, etc.

On February 20 of this year, the European Commission launched a public consultation on its White Paper on Artificial Intelligence, announcing (among other things) its intention to launch a wide-ranging debate on facial recognition technologies. Renaissance Numérique hopes that the concrete proposals put forward in this paper will contribute to an informed public debate and to ensuring the deployment of facial recognition technologies in line with the values that form the cornerstone of the European Union.



ACKNOWLEDGEMENTS

We would like to thank the various actors who took part in the consultations for their contribution, namely:

Didier Baichère, Deputy ("*Député*") for the Yvelines Region

Vincent Bouatou, Director of Innovation, Idemia

Antoine Courmont, Research Officer, CNIL

Théodore Christakis, Professor of International Law, University of Grenoble Alpes

Martin Drago, Lawyer, La Quadrature du Net

Raphaël de Cormis, Vice President of Innovation and Digital Transformation, Thales

Marie Duboys Fresney, Legal Counsel, CNIL

Arthur Messaud, Legal and Policy Analyst, La Quadrature du Net

Henri Verdier, French Ambassador for Digital Affairs

We would also like to thank the office of the *Défenseur des Droits* and the *Ligue des droits de l'Homme* for our constructive discussions on these issues.

Finally, we would like to extend our warmest thanks to the speakers and participants who took part in the symposium on 19 December 2019 at the French *Assemblée nationale*, and especially to Jean-Michel Mis, Deputy ("*Député*") for the Loire Region, with whom we co-organised this event.

FURTHER RESOURCES

"Reconnaissance faciale : Ce que nous en disent les Français", Renaissance Numérique (December 2019)

"Reconnaissance faciale : Interdiction, expérimentation, généralisation, réglementation. Où en est-on ? Où allons-nous ?", summary of the symposium organised on 19 December, 2020 at the French *Assemblée nationale*, Renaissance Numérique (February 2020)

DIRECTOR OF THE PUBLICATION

Henri Isaac, President, Renaissance Numérique

Camille Vaziaga, Head of Public Affairs, Microsoft France

COORDINATION

Jennyfer Chrétien, Executive Director, Renaissance Numérique

Jessica Galissaire, Studies Manager, Renaissance Numérique

AUTHORS

Valérie Fernandez, Professor and Chairholder of the Responsible Digital Identity Chair, Telecom Paris

Jessica Galissaire, Studies Manager, Renaissance Numérique

Léo Laugier, PhD Student in Computer Science, Institut Polytechnique de Paris

Guillaume Morat, Senior Associate, Pinsent Masons

Marine Pouyat, Independent Consultant Expert in Data Protection, marine-talents.com

Annabelle Richard, Associate Lawyer, Technology, Media and Telecommunications Division, Pinsent Masons

THE WORKING GROUP

Sarah Boiteux, Senior Public Affairs Analyst, Google France

Hector de Rivoire, Head of Public Affairs, Microsoft France

Etienne Drouard, Associate Lawyer, Hogan Lovells

Valérie Fernandez, Professor and Chairholder of the Responsible Digital Identity Chair, Telecom Paris

Léo Laugier, PhD Student in Computer Science, Institut Polytechnique de Paris

Guillaume Morat, Senior Associate, Pinsent Masons

Delphine Pouponneau, Director of Diversity and Inclusion, Orange

Marine Pouyat, Independent Consultant Expert in Data Protection, marine-talents.com

Philippe Régnard, Director of Public Affairs for the Digital Branch, La Poste

Annabelle Richard, Associate Lawyer, Technology, Media and Telecommunications Division, Pinsent Masons

Thierry Taboy, Vice President Corporate Social Responsibility, Orange

Amal Taleb, Director of Public Affairs, SAP France

Valérie Tiacoh, Communications Director for Corporate Social Responsibility, Orange

RENAISSANCE
numerique

ABOUT
RENAISSANCE NUMÉRIQUE

Renaissance Numérique is France's main independent think tank focusing on the challenges of the digital transformation of society. Bringing together universities, associations, corporations, start-ups and schools, it aims to develop workable proposals to help public stakeholders, citizens and businesses build an inclusive e-society.

Renaissance Numérique
22 bis rue des Taillandiers - 75011 Paris
www.renaissancenumerique.org

June 2020