FACIAL RECOGNITION

FOR A DEBATE LIVING UP TO THE CHALLENGES

English translation - Only the original French version is deemed authentic

Facial recognition is raising new questions about societal choices and, as such, interest in the subject is growing on national, European and global public agendas alike. In 2018, the CNIL therefore called for attention to be paid to this topic as part of a wider democratic debate on the new uses of video assisted technologies. Today, the CNIL would like to contribute to this debate by presenting the technical, legal and ethical aspects which must, in its view, be borne in mind when addressing this complex issue.

Introduction

Over a year ago now, the CNIL called for a democratic debate to be held on the new uses of video cameras, with a particular focus on facial recognition technologies. Amid an increase in their use and the public authorities' growing awareness of the opportunities and risks they pose, this technology has risen to the top of the public agenda.

This debate is crucial. Indeed, beyond its technicality, political choices have to be made in order to shape what our society will look like tomorrow: given the power of this technology, how can we reconcile the protection of fundamental rights and freedoms with security or economic considerations? Safeguard anonymity in the public space? Define what forms of surveillance are acceptable in a democratic society?

Such choices cannot be made behind closed doors, without democratic control, in fits and starts or by taking ad-hoc initiatives tailored to local contexts, with no overall perspective. Otherwise, there is a considerable risk that these choices will be lost, that gradual shifts will result in unexpected and unwanted societal change and that we will one day be faced with a fait accompli. Political choice should not be dictated simply by technical possibilities. And neither should the political debate be limited to the question of how to make certain digital transformations "acceptable" to our fellow citizens. No. The role of "politics" is to determine which of the possible uses of these technologies are really desirable, leaving the issue of acceptability until the end of the analysis – as a final step rather than as a postulate.

Holding this debate in France also allows our country to contribute from a position of strength to a Europe-wide and worldwide debate, and freely choose its digital society model. In light of the sometimes unfettered and unreasonable uses of facial recognition around the world, we must build a fully-fledged European model. The moratorium adopted in San Francisco – the heartlands of a California at the forefront of digital transformation – symbolises one thing at least: that vigilance, in respect of facial recognition, is not a secondary concern.

This proactive and forward-looking debate must meaningfully address the issues at stake. The CNIL would like to make an initial contribution to this debate today, primarily in terms of method.

To ensure an informed debate, **the terms of the debate must themselves be clear, with an understanding of what facial recognition means.** This will avoid confusion between different uses of this technology where the issues raised are not the same, or with related technologies of a different nature (I). Then, the risks associated **with this technology must be measured,** so that our democratic society can clearly decide which of them it will refuse and which it will assume with appropriate safeguards (II). This debate also falls within a very specific legal framework, within which any use – even experimental – of facial recognition must also fall: the European framework protecting the personal data of our fellow citizens, updated by the General Data Protection Regulation (GDPR) and the Data Protection Law Enforcement Directive of 27 April 2016 (III). Finally, the CNIL wishes to underscore the advisory and monitoring role it plays and will continue to play fully, and independently, in the roll-out of these technologies (IV).

I – Facial recognition: what is it exactly?

The current debate is sometimes distorted by a poor grasp of this technology and of how it exactly works. This can lead to the risks being inadequately described and to confusions between facial recognition and related technologies which also use images at the core of their processing. Another problem arises due to "facial recognition" being referred to in the singular, when it is actually used in many different ways – and the issues involved may vary accordingly, for example in terms of the control people have over their data. By extrapolating from well-established cases of use, there is a high risk of jumping to conclusions about this technology.

1. Facial recognition is a biometric face-recognition technology

Facial recognition is a **probabilistic software application** that can automatically recognise a person based on its facial attributes in order to authenticate or identify them.

Facial recognition falls into the broader category of biometric technology. Biometrics include all automated processes used to recognise an individual by quantifying their physical, physiological or behavioural characteristics (fingerprints, blood vessel patterns, iris structure, etc.). The GDPR defines these characteristics as "biometric data", because they allow or confirm the unique identification of that person.

This is the case with people's faces or, more specifically, their technical processing using facial recognition devices: by taking the image of a face (a photograph or video), it is possible to produce a digital representation of distinct characteristics of this face (this is called a "template"). This template is supposed to be unique and specific to each person and it is, in principle, permanent over time. In the recognition phase, the device then compares this template with other templates previously produced or calculated directly from faces found on an image, photo or video. "Facial recognition" is therefore a two-step process: **the collection of the face and its transformation into a template, followed by the recognition of this face by comparing the corresponding template with one or more other templates.**

Like any biometric process, facial recognition can fulfil **two distinct functions**:

- **the authentication of a person**, aimed at checking that a person is who they claim to be. In this case, the system will compare a pre-recorded biometric template (for example, stored on a smart card) with a single face, such as that of a person turning up at a checkpoint, in order to verify whether this is one and the same person. This functionality therefore relies on the comparison of two templates.

- **the identification of a person**, aimed at finding a person among a group of individuals, in a place, an image or a database. In this case, the system must carry out a test on each face captured to generate a biometric template and check whether it matches a person known to the system. This functionality thus relies on comparing one template with a database of templates. For example, it can link a "civil status" (surname, first name) to a face, if the comparison is made against a database of photographs associated with a surname and first name. It can also involve following a person through a crowd, without necessarily making the link with the person's civil status.

In both cases, the facial recognition techniques used are based on an **estimated match** between templates: the one being compared and the baseline(s). From this point of view, they are **probabilistic.** From the comparison, a higher or lower probability is deduced that the person is indeed the person to be authenticated or identified; if this probability exceeds a certain threshold pre-determined in the system, the system will assume there is a match.

2. Facial recognition is not synonymous with "smart" video

Facial recognition is part of a wider spectrum of video image processing techniques. CCTV systems can film people within a defined area, in particular their faces, but they cannot be used as such to automatically recognise individuals. The same applies to simple photography: a camera is not a facial recognition system because photographs of people need to be processed in a specific way in order to extract biometric data.

The mere detection of faces by so-called "smart" cameras does not constitute a facial recognition system either. While their use also raise important questions in terms of ethics and effectiveness, digital techniques for detecting abnormal behaviours or violent events, or for recognising facial emotions or even silhouettes, are not typically biometric systems.

These examples are not completely unrelated to facial recognition, however. They can be used in conjunction with other systems. Indeed, unlike video capture and processing systems, for example, which require the installation of physical devices, facial recognition is a software functionality which can be implemented within existing systems (cameras, image databases, etc.). Such functionality can therefore be connected or interfaced with a multitude of systems, and combined with other functionalities.

The debate on facial recognition must take this technological continuum into account. We must not use unnecessarily intrusive technologies to tackle specific operational needs, since there may be techniques or measures with a lesser impact that would be equally, if not more, effective. But **the possibility of combining these different systems in practice, with the effect of increasing their impact on people**, must also be considered.

3. Behind the catch-all term, there are multiple cases of use

Facial recognition can be used for a wide variety of purposes, both for commercial purposes and to address public safety concerns. It can be applied in many different contexts: in the personal relationship between a user and a service (access to an application), for access to a specific place (physical filtering), or without any particular limitation in the public space (live facial recognition). It can be for anyone: a customer of a service, an employee, a simple onlooker, a wanted person or someone implicated in legal or administrative proceedings, etc. Some uses are already commonplace and widespread; others are, at this point (in France at least), at the planning or speculative stage, or even absent from the debate altogether.

More specifically, if we look at the range of potential uses, a scale might be considered depending on the degree of control people have over their personal data, the consequences for them (in the case of recognition or non-recognition) and the scale of the processing carried out. Facial recognition based on a template stored on a personal device (smart card, smartphone, etc.) belonging to the person, used for authentication purposes, for strictly personal use and using a dedicated interface, does not pose the same issues as a use for identification purposes, in an uncontrolled environment, without the active involvement of individuals, where the template of each person entering the cameras' field of view is compared with templates from a broad cross-section of the population stored in a database. Between these two extremes lies a very varied spectrum of uses and associated issues.

Some uses are designed for users to have full control over them. **Authentication** can enable **access to services or applications purely in the course of a household activity**, for example. As such it is used extensively by smartphone owners to unlock their device, in place of password authentication.

Facial recognition authentication can also be used to **check the identity of someone hoping to benefit from public or private third party services**. This is the case, for example, with the ALICEM system, which is based on a comparison between a "selfie" and a video taken in real time by the user on one hand, and on the other, the photograph stored in the electronic component of the biometric passport or residence permit belonging to the same person. This process thus offers a way of creating a digital identity using a mobile app (smartphone, tablet, etc.) which can then be used to securely access online administrative services.

As far as accessing commercial services is concerned, biometric authentication can be harnessed to open a bank account remotely for example. In this case, the biometric template calculated by processing an identity photograph submitted by the bank customer is compared with a photographic self-portrait of that person.

Authentication can also be used to **control physical access** to one or more predetermined locations, such as entrances to buildings or specific crossing points. This functionality is, for example, implemented in the PARAFE processing of border crossings, where the photograph of the person at the checkpoint device is compared with the one stored in their identity document (passport or secure residence permit).

Identification can be applied in many, even more diverse ways. These particularly include the following uses, currently observed or planned in France or other parts of Europe:

- **automatic recognition of people in an image** to identify, for example, their relationships on a social network such as Facebook, which uses it. The image is compared with the templates of everyone on the network who has consented to this functionality in order to suggest the nominative identification of these relationships;
- **access to services**, with some cash dispensers recognising their customers, by comparing a face captured by a camera with the database of faces held by the bank;
- **tracking of a transport service passenger's journey** at each stage of the journey. The template, calculated in real time, of any person checking in at gates located at certain stages of the journey (baggage drop-off points, boarding gates, etc.), is compared with the templates of people previously registered in the system;
- **searching,** in a database of photographs, **for the civil status of an unidentified person (victim, suspect, etc.)**. This is done with the TAJ system (the processing of criminal records file in France) for example;
- **monitoring of a person's movements** in the public space. Their face is compared with the biometric templates of people travelling or having travelled in the monitored area, for example when a piece of luggage is left behind or after a crime has been committed;
- **reconstructing a person's journey** and their subsequent interactions with third parties, through a delayed comparison of the same elements in a bid to identify their contacts for example;
- **identification of wanted persons in public spaces.** All faces captured live by video-protection cameras are cross-checked, in real time, against a database held by the security forces.

These are only examples of applications or projects currently observed or planned in France and Europe, for which compliance with the legal framework may not therefore have been assessed yet, in particular for some of the identification systems afore mentioned. Yet potential use of facial recognition is even much wider. As a matter of fact, some other countries use facial recognition to enforce traffic offences concerning pedestrians via CCTV surveillance, or to combat fraud. Others even automatically identify everyone moving along in public spaces.

In this context, a use-by-use approach must be applied. This methodology has been required since 1978 in France and was reaffirmed in 2016 at the European level by the fundamental texts on data protection: to determine whether the processing of personal data is lawful, it is necessary to start from its purpose, from the aim pursued. It is only in the context of a specific purpose that it is possible to assess whether the data is relevant and proportionate, whether the retention periods are appropriate, whether security is adequate, etc. **What this means is that, although there may be lawful and legitimate cases for the use of facial recognition, it should not be considered desirable or possible in all cases**.

II - The impacts of facial recognition: what are the risks of this technology?

The risks actually posed by this technology need to be accurately assessed in order to manage them effectively and even refuse certain uses. The GDPR and French Data Protection Act may well be "technologically neutral" texts, but their application in practice should not ignore the significance of these risks, from those shared with other biometric techniques to the more specific risks of facial recognition, such as the decline of anonymity in the public space.

1. Highly sensitive data that are subject to special protection

Data protection legislation defines biometric data as "sensitive" data, just as data concerning health or sex life, political opinions and religious beliefs or genetic data. **This shows a new stance on the part of the European legislator**: biometric data processing did not used to be classified as sensitive, but the GDPR and Data Protection Law Enforcement Directive have revised its status to take full account of the risks posed in its processing.

Like other sensitive data, biometric data **relates to people's privacy**. It is distinctive in that it allows the data subject to be identified at any time based on **a biological fact specific to them, permanent over time and from which they cannot be dissociated**.

Unlike any other personal data, biometric data is not attributed by a third party or even chosen by the data subject: it is produced by the body itself and designates or represents it and it alone, in an immutable way. Therefore, it cannot be considered as a password or a login, which can be changed if compromised (loss, system intrusion, etc.): it is **non-revocable**. Any misappropriation or misuse of this data thus entails substantial risks for the person from whom it originates: denial of access to services or places, identity theft for fraudulent or even criminal purposes, etc.

Like other biometric techniques, facial recognition is therefore never a completely harmless type of processing. Even legitimate and well-defined use can, in the event of a cyber-attack or a simple error, have particularly serious consequences. In this context, the question of **securing biometric data** is crucial and must be an overriding priority in the design of any project of this kind. The storage of biometric data on a personal device belonging to and accessible to the user should always be prioritised over central database storage solutions, in order to minimise the risks involved. Only in cases of absolute necessity and in the absence of any alternative may centralised storage be considered, subject to strict security measures.

For these reasons, biometric processing, including facial recognition, is subject to a strict legal framework that has been reinforced by recent European texts. In the GDPR, the principle is to prohibit such processing. These data may only be processed, by way of exception, in certain specific cases (with the explicit consent of individuals, to protect their vital interests or on the basis of a substantial public interest) and with appropriate safeguards adapted to these risks. The Data Protection Law Enforcement Directive follows the same logic, only allowing such data to be processed in cases of absolute necessity. The French Act of 20 June 2018, amending the Data Protection Act, is in line with European texts. In the absence of consent, an operator, whether public or private, may only implement biometric processing if it has first been authorised by law.

2. A contactless and potentially ubiquitous technology

Unlike other data which is processed biometrically, **facial recognition data can, potentially, be obtained everywhere.** People's faces are collected and registered in a multitude of widely available databases, which thus keep track of people's movements through time and space, therefore constituting a potential source of comparison for any facial recognition system. More generally, any photograph can potentially become a piece of biometric data with more or less straightforward technical processing.

This dissemination of data used by facial recognition devices is also taking place amid a context of permanent self-exposure on social media and, more generally, of porosity between household, private and public uses of this data. This gives us an idea of the sheer amount of data that is technically accessible and can potentially be mobilised for facial recognition-based identification. Facial recognition is altogether specific in this respect.

Facial recognition can also be used as a **"contactless" system,** with some devices completely removing the machine from the user's field of vision. It **allows the remote processing of data without a person's knowledge.** This is not the case for all uses (unlocking a smartphone, and, more generally, most authentication uses), but it can allow real-time tracking of everyone's movements, without any interaction with the person and therefore without their even being aware of it. From a technical point of view, facial recognition thus allows what no other technology currently allows or has ever allowed: recognition of a person without any action on their part – either at the time of registration or comparison – or even identification of such a person by name, without the owner of the device ever having had any relationship with that person.

At a time when the advantages of "seamless" technologies and "fluidity of services" are being extolled, it should be remembered that some form of conscious interaction or effort can be useful. This can help to **remind people of the reality and consequences of their interactions with digital tools**. It can also provide an opportunity for people to assert their rights.

3. An unprecedented surveillance potential, capable of undermining societal choices

Facial recognition systems can interface easily with all sorts of video devices. **There are already many image-capture devices embedded in our day-to-day routines.** Video surveillance devices, smartphones and advertising screens are all examples of systems that could potentially be turned into tools for an unprecedented level of surveillance – in the generic sense of the term (sovereign or private). It is not unthinkable that these image-capture devices, which are potentially compatible with any facial recognition system, might also be coupled with other types of technology, such as sound capture – which would further increase the level of surveillance of people and places. This technological shift is happening in tandem with a **shift of the surveillance paradigm**, already in evidence in many areas, where **targeted surveillance of certain individuals has progressed onto a massive surveillance for the purposes of identifying certain individuals**. The replacement of humans with algorithmic processing to carry out identity checks is in itself altering the potential for surveillance. The changing nature of surveillance, which is becoming indiscriminate, can, moreover, be seen in the use of facial recognition in the public space via video surveillance cameras. Identifying a person in public spaces requires the biometric processing of everyone moving along in the public space under surveillance – templates must be generated for everyone in order to find the wanted person by comparison.

The most advanced uses of facial recognition therefore pose an obvious risk to **anonymity in the public space**. Whether physical or digital, the public space is somewhere many individual and public freedoms are exercised, including the right to privacy and personal data protection, the freedom of expression and assembly, the right to protest, the freedom of conscience and the freedom of religion. This anonymity is protected by law: there is no rule that says everyone must be identified or identify themselves whenever they move in the public space. While there are some prohibitions in this respect (ban on concealing one's face) and some obligations (such as wearing a badge in certain places or being required to submit to controls, verifications and identity checks), these measures are specifically regulated by law and in no way undermine the possibility for anonymity in public spaces. Erosion of this anonymity, by public authorities or private organisations, is thus likely to jeopardise some of our fundamental principles and therefore calls for careful consideration.

Feedback, particularly abroad, shows that facial recognition in the public space can end up making harmless behaviour look suspicious. Wearing a hood, sunglasses or a cap, looking at your telephone or at the ground, can have an impact on the effectiveness of these devices and serve as a basis for suspicion in itself.

All of these impacts must be weighed carefully, since some technological developments may well end up quietly redefining how we are allowed to behave in society.

4. Fallible and costly technologies that require a clear and comprehensive assessment

Like any biometric processing, facial recognition is based on statistical estimates of the match between the elements being compared. It is therefore inherently fallible. The response provided by a biometric comparison system is never binary (yes or no); it is a probability of match. Furthermore, the biometric templates calculated are always different depending on the conditions under which they are calculated (lighting, angle, image quality, resolution of the face, etc.). Every device therefore exhibits variable performance according, on the one hand, to its aims, and, on the other hand, to the conditions for collecting the faces being compared.

Like other similar techniques, facial recognition thus inevitably leads to "false positives" (a person is wrongly identified) and "false negatives" (the system does not recognise a person who ought to be recognised). Depending on the quality and configuration of the device, the rate of false positives and false negatives may vary. Moreover, these settings can lead to knock-on effects which need to be borne in mind. Imagine that precedence is given to reducing "false negatives", for national security purposes (such as counter-terrorism). This may end up increasing the number of "false positives", i.e. people who are likely to be wrongly identified as suspects (with the downsides that this entails). **This variation in performance can thus have far-reaching consequences for people who are mis-identified by the device.** The practical questions this raises need to be taken seriously for defining applications and the measures to be implemented as a result. Operators' choices when configuring these systems are therefore of the utmost importance.

Furthermore, **there is a significant element of bias inherent in this technology**: trials conducted in France and other countries have, for example, demonstrated that the error rates of facial recognition algorithms can vary with gender or skin colour. Even if steps – not least the self-configuration of algorithms – can be taken to reduce such bias, the very nature of biometric processing, regardless of the degree of maturity of the technology, means that bias will inevitably continue to be observed.

These **insurmountable technical limitations** can seem at odds with the hype and fascination surrounding a technology that is sometimes wrongly perceived or presented as infallible. And yet they must be factored into the necessary investment choices, in both budgetary and societal terms, when considering whether or not to use facial recognition.

The **economic cost** of facial recognition devices must be very accurately documented in this respect. It most often rests with public authorities or local government, in a global context of streamlining public expenditure, without the return on investment always being measured accurately or methodically. These costs (installation of physical devices, development of very high computing power, installation of servers, storage capacity, software costs, maintenance and upgrade costs, etc.) cannot be underestimated and decisions taken in this respect therefore inevitably call for the allocation of new resources or rechanneling of resources away from other devices.

III - Should we experiment with facial recognition? Within a defined framework and methodically

Public authorities are seemingly considering developing facial recognition through an experimental approach. Three key requirements must guide this process, not only to ensure respect for the principles protecting citizens' privacy and personal data but also to inspire trust in any systems that are implemented.

1. First requirement: draw some red lines, even before any experimental use

Facial recognition, whether experimental or not, must respect the European framework, GDPR and the Data Protection Law Enforcement Directive. Within this framework, **not everything is or will be allowed** where facial recognition is concerned. The purpose of the experimentation is, undoubtedly, to draw the boundaries defining the scope of what is desirable (politically, socially, etc.), and the scope of what is possible (technologically, financially, etc.). **Some boundaries already exist**, however. The debate, as praiseworthy as it is, cannot be informed by all types of trial.

The CNIL has already had the opportunity to recognise the legitimacy and proportionality of some uses. For example, and without prejudice to its assessments concerning some implementation methods (particularly the free nature of consent obtained in respect of the ALICEM device), in the case of the PARAFE and ALICEM devices, it has allowed facial recognition to be used where there is a need for a particularly high level of authentication of individuals and on condition they have control over their biometric data. During the Nice carnival, it also allowed facial recognition technology to be tested under real conditions on a sample of volunteers, with no operational implications, to filter access to the carnival area.

The CNIL has also already pointed out that certain uses are forbidden in our society. It has recently made this clear with regard to implementing facial recognition authentication systems for children for the purpose of controlling access to schools – when the aims of securing and facilitating entry to schools can be achieved by equally effective but much less intrusive means in terms of privacy and individual freedoms, taking into account the special protection that children must be afforded.

Other projects may thus have to comply with these more stringent requirements. The principles of the legitimacy of the aims pursued and the strict necessity of implementing such biometric processing are indeed indispensable requirements. Facial recognition cannot be lawfully used – even on an experimental basis – unless it is grounded in a specific requirement to ensure a high level of reliability in the authentication or identification of data subjects and without demonstrating the inadequacy of other, less intrusive security means.

The proportionality of the means deployed in relation to aims deemed to be legitimate is also an indispensable requirement. In this respect, live facial recognition, which is based on the indiscriminate capturing of faces in a specific space, calls for special vigilance. Given its scope and the degree of surveillance it involves, this type of use calls for a thorough analysis, in each context of use and on an aim-by-aim basis, in order to assess the adequacy or the inadequacy of such identification systems. Protecting the rights of children and other vulnerable people is also an overriding condition.

If development of an experimental framework for facial recognition is decided on, this should provide an opportunity, with guidance provided by the CNIL in its role as advisor to the public authorities, to fix these red lines beyond which no use, even experimental, can be allowed.

2. Second requirement: put respect for people at the heart of the approach

Data protection and privacy are fundamental rights, which encompass a series of more specific rights in practice: the right to information, the right to object, the right to rectification, the right not to be subject to a fully automated decision, etc. In the digital age, people have a growing desire to know who is processing their data and how, in order to "keep the upper hand" over what happens to it. The CNIL sees more evidence of this every day. In light of the major impacts that facial recognition devices have on people, **respect for their rights is of particular importance and must be central to the approach.**

Accordingly, people's **consent** must be obtained for each device that allows it, particularly in the context of trials. Data **control**, through devices owned by individuals and over which they have full control, must be given priority. **Transparency** for individuals must be ensured in all circumstances, by providing clear, comprehensible and easily accessible information. Their **rights** to withdraw their participation to the processing, to access information concerning them and to have recourse to human intervention in the case of automatic controls, must be guaranteed. The **security** of their biometric data, relating to individual privacy (which, if compromised, may have serious consequences for their daily lives), should be an overriding condition underpinning their processing.

Apart from legally recognised rights, people themselves must be put at the heart of any facial recognition system. **Experimentations should not have the ethical purpose or effect of accustoming people to intrusive surveillance techniques**, with the more or less explicit aim of preparing the ground for further deployment. At this stage, there should be no question of making devices, which weaken people's autonomy or violate their fundamental rights, "acceptable". Acceptability can only become an aim once devices have been recognised as perfectly legitimate and lawful.

3. Third requirement: adopt a genuinely experimental approach

Given the issues posed by facial recognition, it is imperative to protect against any ratchet effect associated with implementing some devices. From this point of view, an experimental approach is undoubtedly preferable to creating a permanent framework from the outset, which would establish a number of generally authorised uses in France. Nevertheless, the deployment of these systems must then follow a genuinely experimental approach.

This particularly involves limiting such devices in time and space and precisely identifying what these experimentations are setting out to achieve and their criteria for successful deployment. Precise definition of their assessment methods, which must be rigorous, adversarial, multidisciplinary and carried out within a reasonable timeframe, as well as determination of the authorities responsible for it, are key aspects. Comparison with other technical devices capable of meeting the same needs will furthermore lead to a better assessment of facial recognition systems.

The legal framework must therefore guarantee the fairness of the trials carried out, the outcome of which should not be prejudged. To that end, it must establish a rigorous experimental methodology, based on the more general legal framework in this area and on the "methodological guide" recently drawn up by the Council of State. This is to ensure full advantage is taken of such an approach while exercising the necessary caution with regard to the risks posed by facial recognition.

Such caution is not intended to restrict technological innovation. On the contrary, **with a genuinely experimental approach it will be possible to test and perfect technical solutions that respect the legal framework**, when they arise, and which directly integrate the constraints associated with these rules.

IV - What role will the CNIL play in regulating facial recognition?

In 2016, the GDPR and Data Protection Law Enforcement Directive enshrined the principles of protecting freedoms, privacy and personal data at European level. These principles resonate with a "Republican pact on digital technology" recalled in Article 1 of the French Data Protection Act: "*Information technology should be at the service of every citizen. [...] It shall not violate human identity, human rights, privacy, or individual or public liberties*".

In this instance, the purpose of this pact is not to futilely set data protection, on the one hand, against the legitimate aims of some facial recognition projects (security, provision of a digital identity, etc.) on the other. It is to encourage efforts to find a way to reconcile these two sets of requirements over the long term, at the same time focusing on the ethical issues that come with any digital transformation.

Political choices are the responsibility of the Government and Parliament. Regardless of the choices made, the **CNIL will play its role as independent guarantor of these meaningful principles, through its dual mission of advising the public authorities and, as far as necessary, enforcing compliance with the law**.

In this regard, it must at each stage ensure compliance with the specific rules established by the current legal framework on biometric data processing. These now apply to all facial recognition devices and include: strict exceptions to the principle of prohibiting the processing of such data, free and informed consent of individuals participating in a biometric system, performance of an data protection impact assessment prior to the implementation of such processing in order to limit the risks and the necessary regulation by legal texts, adopted after consulting the CNIL, of devices which do not require consent from individuals.

If an ad-hoc experimental facial recognition device should emerge, **the CNIL will advise the public authorities on any experimentation framework** (scope, method, substantive rules, etc.) beforehand and will have to be consulted on any draft legislative or regulatory text aimed at allowing or facilitating experimentations.

It could also be systematically consulted in advance on specific planned experimentations. In this way it could ensure that proposed facial recognition systems comply with the experimental legal framework thus established and draw attention to the aspects which, from a data protection point of view, must undergo specific assessment. During such consultations, the CNIL must have access to the impact assessments drawn up before each processing operation is carried out. It must in any case **be provided with periodic reports**, at each stage and at the end of the trial, in order to be able to contribute to the assessment of these devices. Of course, the CNIL will remain free at any time to exercise all of its powers allowing it, on its own initiative or at the request of the persons concerned, to **monitor compliance in practice with the legal framework and, if necessary, to impose the necessary corrective measures** or even call for unlawful devices to be removed.

In performing all of its missions, the CNIL will remain completely independent. It cannot therefore play an active part in the effective organisation of facial recognition trials or their management. In this way it will be able to assume its role as regulator to the full.