Facial recognition: for a debate living up to the challenges

19 December 2019

Facial recognition is raising new questions about societal choices and, as such, interest in this technology 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.

Facial recognition calls for political choices to be made: on the role we give this technology, on how it affects the fundamental freedoms of individuals, and on what our place is in the digital age. These choices will shape what our society looks like tomorrow. The debate must not therefore be limited to a technical consideration of the potential uses and effectiveness of this technology. Nor should it solely be aimed at finding out how to make acceptable to citizens a technology which would be necessary. It is indeed not the case: it's a complex issue, and one that warrants a lucid and in-depth debate. The purpose of this debate is therefore to determine in which cases facial recognition is necessary in a democratic society, and in which cases it is not.

The debate surrounding this technology must therefore be proactive and forward-looking, in order to keep the upper hand over the model of society we want. The aim is to avoid any change of society only through the gradual accumulation of new uses of this technology, through its insidious creeping into citizens' daily lives, and without this change having first been the subject of a comprehensive debate and a conscious political choice.

This is why the CNIL, drawing on its expertise in facial recognition and as guarantor of the "Republican pact on digital technology" enshrined in the French Data Protection Act and GDPR, would like to make an initial contribution, in terms of method, to this debate. This contribution, reviewed by CNIL Commissioners on 7 November 2019, has **four aims**:

- **To present, in technical terms, what facial recognition is and what it is used for,**

in order to ensure the subject of the debate is clear for all. This biometric technique for the automated recognition of a person, based on the characteristics of their face, should not be confused with other image processing techniques (such as "smart video" devices that detect events or emotions but yet do not recognise individuals), with which it can sometimes be combined. Above all, behind the catch-all term "facial recognition" are a host of possible uses, from unlocking smartphones to opening bank accounts, to recognising a person being sought by police in a crowd. These uses do not all raise the same issues, particularly in terms of people's control over their data.

This balanced overview is necessary in order to avoid any confusion and any blanket conclusion on this technology. On the contrary, it is necessary to reason on a use-by-use basis.

- **To highlight the technological, ethical and societal risks associated with this technology.**

These risks are linked to the biometric nature of facial recognition: the data extracted from faces concerns the body, and individuals' privacy. Any data breach or misuse would pose significant risks (blocking of access to a service, identity theft, etc.). Facial recognition is furthermore based on a probability rather than on the absolute certainty of a match between the faces being compared and the baseline "template". Variations in performance can therefore have far-reaching consequences for individuals who are mis-identified.
Another issue is that this technology allows remote, contactless, data processing, even without a person's knowledge. In the current digital environment, where people's faces are available across multiple databases and captured by numerous cameras, facial recognition has the potential to become a particularly ubiquitous and intrusive tool. The increased surveillance enabled by this technology may ultimately reduce the level of anonymity afforded to citizens in the public space.

This risk assessment is necessary to determine which risks are not acceptable in a democratic society and which ones can be assumed with appropriate safeguards.

- **To recall the framework governing facial recognition devices and their experimentation.**

European (GDPR, Data Protection Law Enforcement Directive) and national (amendments to the French Data Protection Act in 2018) legislators have very recently introduced more stringent rules on biometric devices with the aim of bringing data protection in line with the new uses of digital technology. Any use, including experimental, of facial recognition must therefore respect this updated legal framework.

In accordance with these rules, the need for such devices must be established on a case-by-case basis: facial recognition cannot be used without a specific requirement to ensure high reliability in verifying the identity of individuals. These texts also require that the proportionality of the means deployed and the special protection afforded to children be both guaranteed. They call for respect for people to be at the heart of the systems, for example by obtaining their consent or by ensuring they have control over their data. It is by applying these principles, recently reaffirmed at European level, that the CNIL has already had the opportunity to allow certain uses in principle, while regulating them in practical terms (border control at airports), and to refuse others (controlling student access in schools).

These more stringent requirements will apply to any framework, even experimental, for facial recognition systems.

- **To clarify the CNIL's role in any experimentations of new facial recognition devices.**

The CNIL is neither a decision-maker nor a prescriber in this area: the choice of such a framework, its nature and scope, rests with the Government and Parliament.

European and national law has, however, vested the CNIL with advisory missions, for public authorities in particular, and monitoring missions. It intends to fully assume its role with respect to this technology, not least by providing independent advice on the legal and methodological framework governing an experimental approach. It will also be able to advise project leaders on the trials planned and contribute, within its sphere of competence, to the assessment of these devices. If necessary, the CNIL will exercise its powers of investigation on these devices by taking any corrective measures necessary to protect people. In carrying out all of its missions, the CNIL will remain fully independent.