



AI-REGULATION.COM

27/11/2020

French White Paper on Internal Security Makes Several Proposals for the Use of Facial Recognition in France

Theodore Christakis and Anaïs Trotry

▶ To cite this article:

Theodore Christakis and Anaïs Trotry, French White Paper on Internal Security Makes Several Proposals for the Use of Facial Recognition in France, Chair Legal and Regulatory Implications of Artificial Intelligence, MIAI Grenoble Alpes, November 27th 2020.

[AI-Regulation.com](https://www.ai-regulation.com)

CHAIR LEGAL AND REGULATORY IMPLICATIONS OF ARTIFICIAL INTELLIGENCE

A very important [White Paper on Internal Security](#), published on November 16, 2020, by the French Ministry of the Interior, makes several proposals for the use of Facial Recognition Technology (FRT) by public authorities in France.

The White Paper on Internal Security is a forward-looking document, which contains nearly 200 proposals, based on what it calls the “internal security challenges” of the 21st century. It succeeds to the previous “White Paper on Public Security”, published in 2011.

The fourth booklet of White Paper on Internal Security, entitled “Bringing the Ministry of the Interior to the Technological Frontier”, addresses issues around new technologies and devotes two specific parts to the use of FRT. This brief post will present briefly these FRT-related proposals, while a separate post will present other AI-related proposals in the White Paper.

1) Consolidating the Forensic Use of Face Recognition

The first set of FRT-related proposals concerns the use of face recognition as a tool for identifying suspects (for instance on the basis of a photo or video-still) within the context of criminal investigations (see pages 258-260).

The White Paper first highlights that “identification matching” (*rapprochement en identification*) is technologically possible and has been legal in France for almost ten years, and goes on to say that article R. 40-26 of the Code of Criminal Procedure permits its use within the TAJ. It should be reminded that the TAJ (“*Traitement des antécédents judiciaires*”) is a database, used in the context of judicial and administrative investigations, which contains data collected in the course of proceedings and in particular photographs containing technical characteristics that can also be used by facial recognition systems. The White Paper states that the field in which facial recognition technological advances will be “the most immediately exploitable for internal security services” is that of forensics.

The paper states that improving the quality of the photographs contained in the TAJ and developing technology capable of capturing and processing facial biometric images is essential to increasing the proportion of solved cases. The White Paper therefore proposes that a complete review of these photographs be undertaken in order to determine a methodology for progressively improving their quality. It also makes other proposals in relation with the composition and use of the relevant databases.

2) Experimenting with Facial Recognition in Public Spaces

The White Paper considers that experimenting with facial recognition in public spaces would be “highly desirable” in order to test out FRT technically, operationally, and legally, as well as to ensure that the French people are protected (see pages 263-265).

The paper notes several reasons for an acceleration in the development of FRT, including the fact that FRT performance is improving significantly. It highlights that the FRT error rate, despite a progressive reduction, appears nevertheless to be substantial. Therefore, it

emphasises that human control remains essential to eliminating residual false positives and avoiding negative consequences for people.

The White Paper then emphasises the importance of “prior experiments”, which would allow for the deepening of certain FRT parameters. Accordingly, three axes of experimentation are proposed:

- The first axis consists of a comparison of the potential of diverse types of sensors (fixed sensors, tactical sensors, drones...) on which FRT could rely.
- The second axis concerns the intended purposes of the FRT, which may be either strictly judicial or incorporate preventive purposes “for highly serious reasons”, such as the prevention of terrorism or serious crime.
- The third axis relates to potential uses of FRT in terms of identification, such as the protection of sensitive buildings/venues against terrorist attacks or the identification of wanted individuals.

The White Paper also states that experimenting with facial recognition could eventually be extended to non-state operators for tracking purposes, provided that they are strictly time and space limited, for example to locate the owner of lost property in a train station or airport.

The White Papers emphasises that experimentation with facial recognition should be gradual, and that a certain degree of technical and operational control will have to be guaranteed before legal consequences for those identified can proceed. Accordingly, the paper presents a three-phase methodology to support and provide the basis for these experiments:

- The first phase would consist of a "blank" experiment based on voluntary grounds. The FRTs would be deployed in a restricted area and reserved for an informed public who have the ability to avoid experimentation.
- The second phase would be to deploy the FRT under real conditions. It would only be activated after verification that the technical parameters of error are limited and adequately manageable by a human process. This experiment could take place in a real situation, but the phase would however include a warning to the public, so as to assess the dissuasive effect (or not) of the technology.
- The third phase, “based on public interest”, would consist of a series of geographically and temporally limited experiments, under real conditions and without prior information to the public. This phase would allow for the assessment of the concrete contribution of FRT “to the identification of wanted or watched people”.

The paper notes that a new phase would only take place if the results of the previous phase are positive and conclusive.

Highlighting concerns raised about FRT, the White Paper asserts that these experiments should be time-bound and carried out in a transparent manner. Therefore, the composition of the “reference lists”, or “watchlists”, should be submitted either to the judicial authority or to an independent administrative body (depending on the legal regime) during the experiment. Furthermore, an independent body, which would publish its own analysis to inform public debate, should have permanent access to the progress of the experiment throughout its duration.

The White Paper also suggests seizing the opportunity presented by facial recognition experiments to test the deployment of image analysis techniques based on artificial intelligence in operational situations.

Finally, the White Paper on Internal Security emphasises that FRT must be used for the protection of populations and sensitive sites, and be based on the principles of necessity, legality, proportionality and control.

Reminder: the French DPA CNIL’s Position on FRT “Experiments” by Public Authorities

These proposals on FRT “experimentations” in public spaces come against the background of a rather cautionary approach adopted on such experimentations by the French Data Protection Authority (CNIL). In November 2019 CNIL published a [report](#) on facial recognition, presenting various technical, legal and ethical issues that must be taken into account. The CNIL specifically discussed the legal framework within which experiments and deployments of FRT may be carried out.

The French DPA, recalled that FRT, whether experimental or not, must respect the European framework (especially the [GDPR](#) and the 2016 [Law Enforcement Directive](#)) and highlighted three key requirements which must guide any FRT experimental approach.

A) First requirement: Draw some red lines, even before any experimental use

The CNIL stated that “not everything is or will be allowed” where FRT is concerned. Some uses appear legitimate and proportionate, while some others are forbidden, such as implementing FRT to control access to schools (for this question see also the position of the Supreme French Administrative Court in [our article here](#)).

It emphasised that the proportionality of the means deployed, the legitimacy of the aims pursued and the necessity of implementing such biometric processing are “indispensable”. It also stated that FRT cannot be lawfully used, even on an experimental basis, “without demonstrating the inadequacy of less intrusive security means” and “unless grounded in a specific requirement to ensure a high level of reliability” in the identification of individuals.

Highlighting that “live facial recognition”, based on the indiscriminate capturing of faces in a specific space, calls for “special vigilance”, the CNIL noted that such use of FRT calls for a thorough analysis in order to assess the adequacy or the inadequacy of such identification systems.

B) Second requirement: Put respect for people at the heart of the approach

Highlighting the major impacts that FRT have on people, the French DPA emphasised the importance of respecting fundamental rights, such as data protection and privacy, in the context of FRT experimentation. Accordingly, “people’s consent must be obtained for each device that allows it”, and “transparency for individuals must be ensured” in all circumstances, by “providing clear, comprehensible and easily accessible information”.

The CNIL also noted that the security of biometric data should be guaranteed, and that experiments should not have the “effect of accustoming people to intrusive surveillance techniques, with the more or less explicit aim of preparing the ground for further deployment.”

C) Third requirement: Adopt a genuinely experimental approach

The French DPA stated that experimenting FRT is undoubtedly preferable to “creating a permanent framework from the outset”. It stressed, nonetheless, that the deployment of FRT must follow a rigorous experimental approach, which suppose a temporal and geographical limitation and a clear identification of intended purposes and success criteria.

According to CNIL, accurately determining the responsible authorities and comparing FRT with other technical devices capable of meeting the same needs are both key aspects, as well as precisely defining the assessment methods “which must be rigorous, adversarial, multidisciplinary and carried out within a reasonable timeframe”.

In addition to the measures advocated by the French DPA, researchers of the National Institute for Research in Computer Science and Control (INRIA) recently published a [detailed methodology](#) which appears complementary to the CNIL report. Proposing a systematic approach for analysing the impacts of FRT, the authors emphasised that FRT experiments must be subject to an impact assessment, be limited in time and follow a rigorous protocol.

These statements are attributable only to the author, and their publication here does not necessarily reflect the view of the other members of the AI-Regulation Chair or any partner organizations.

This work has been partially supported by MIAI @ Grenoble Alpes, (ANR-19-P3IA-0003)