The CREOGN Research Notes

French Gendarmerie Officers Academy Research Centre

Issue 43 – September 2019

Colonel Dominique SCHOENHER

CREOGN
CENTRE DE RECHERCHE

FACIAL RECOGNITION AND PREVENTIVE CONTROLS ON THE PUBLIC HIGHWAY, THE CHALLENGE OF ACCEPTABILITY

The CREOGN had already addressed this issue in early 2016[1] , an eternity in technological terms. At the time, the reliability of technical solutions was highly questionable and their public use remained marginal.
Today, facial recognition technology has become commonplace in commercial use and is becoming more mature every day for public safety use. It is already deployed and openly accepted as a means of surveillance across a large scale country like China. However, as with any use of technology for security purposes, controversy is rife as to its potential abuses, its real effectiveness and its degree of infringement on individual liberties. Indeed, while the French population is willing to use facial recognition in their daily lives as consumers, a practice that some sociologists believe helps to desensitize them[2] , they are not ready to accept its unconditional use by law enforcement agencies. The Vichy regime and its identity registration system have left such a deep scar on French society's collective memory that any form of state registration will inevitably trigger instinctive, outright rejection. Moreover, there's no denying that a person's face is unlike any other biometric data. It is at the heart of our social interactions, it is our permanent calling card in the physical world[3] , our main means of expressing our emotions, much more sincere than language.
In order to go beyond purely ideological postures, the use of facial recognition by law enforcement agencies deserves to stem from an enlightened societal choice based on technical guarantees and on a consolidated law allowing for scientific experimentation.

I) From policing Grail to dystopia, a political and societal choice

If it ever does reach an acceptable level of reliability, the added value of this technology for law-enforcement will be indisputable. It is the culmination of the anthropometric forensic approach begun 150 years ago to identify troublemakers, the most dangerous of whom were previously branded with a red-hot iron. The interest of this technology is to systematically and automatically carry out such basic policing actions as identification, tracking and search for individuals, while rendering those actions invisible. Provided that the algorithms are free of bias, it could put an end to years of controversy about racial profiling since identity checks would be permanent and apply to all[4]. In the same way, it would allow for greater reactivity when searching for missing vulnerable persons or tracking down criminals on the run. It may also induce a form of self-monitoring which would curb anti-social

1 CREOGN Research Note – Issue 18, April 2016. https://www.gendarmerie.interieur.gouv.fr/crgn/Publications/Notes-du-CREOGN/Numerisation-du-visage-opportunites-et-limites-de-la-reconnaissance-faciale

2 Asma Mhalla (Lecturer at Sciences Po) : « Nous manquons de réflexion éthique sur l'IA et la reconnaissance faciale », « L'empire du signal, ou les dangers d'un contrôle social par les corps »

3 Depending on practices, that observation can apply to the virtual world (selfie trend, tagging people on photos and even emoticons) but some prefer using other faces (avatars)

4 This would yet be subject to a change in Conseil Constitutionnel case-law, as its decision n° 93-323 DC from 5 August 1993 stated that the practice of generalized and discretionary identity checks would be incompatible with the respect of individual freedom.

behaviour (non-compliance with road rules, animal waste disposal, garbage dumping), as exemplified by the Chinese social credit model[5].

Such promises of efficiency should not mask the potential totalitarian drifts within a State that would like to exploit it to ensure permanent social control over its population and repression against individuals or groups deemed dissident. History has shown that no country is immune to authoritarian drift. Even if France were, another danger could come from constant espionage by a foreign power, should the technology not be mastered in all its components[6]. This harmful potential, reinforced by the convergence of technologies and the multiplication of connected objects in our environment as sources of new video streams that can feed facial recognition systems, will make the notion of anonymity in the public space obsolete. Without regulation, the prediction of American prospectivist Howard Rheingold will come true[7].

Facial recognition cannot be "uninvented"; it has already flourished in private and commercial uses. However, the much-discussed bans on the use of facial recognition by the municipalities of San Francisco, Somerville and Oakland in the United States, which are being considered by certain States such as California and which presidential candidate Bernie Sanders would like to extend to the federal level, have had the merit of fueling the debate[8]. Yet, this debate cannot currently be taking place in France, as the population and its representatives are not sufficiently informed about the challenges of facial recognition. Even though press articles, generally Manichean, are multiplying, there are few French studies or surveys on the acceptability of biometric technologies. A 2013 study by the Centre de recherche pour l'étude et l'observation des conditions de vie *(Research Center for the Study and Observation of Living Conditions)* showed that people approved of uses for security purposes but rejected commercial uses (a situation which is the exact opposite of our current reality) and set up prior individual consent as a sine qua non condition. That same year, an IPSOS poll mentioned that 72% of respondents were in favor of video protection coupled with facial recognition-enhanced video protection (65% among 15-24 year olds). An ODOXA poll in June 2017 raised this rate to 85% for the detection of people listed on a security services watch list during major events[9].
Although rare, these polls agree on three points. Young people and minorities intuitively feel more threatened by the misuse of facial recognition. Facial recognition only receives overwhelming support when it is intended to reduce a serious risk that is clearly defined in terms of time and space . The prior consent of the citizen, and not only his or her information, appears to be a condition for its legitimate and legal use[10] on the public highway.

Beyond these statistical observations, which factors would bring about the support of the French population and convince them that such a tool is harmless in the hands of the State?

II) The prerequisite : a reliable and secure technology

Reliability is the first source of trust in technology. The case of the autonomous car shows us that the social acceptance threshold of error is very low for processes driven by artificial intelligence[11] , even more so for those that affect individual liberties.

5 China has put in place a rating system that assesses its population's behavior leading to stigmatizing measures (traveling or loan-approval restrictions) for nearly 23 million individuals whose social credit ranks low.

6 This is clearly illustrated in the debates around HUAWEI equipment for the deployment of 5G. It would be the same for the algorithms implemented.

7 When observing the political, social and economic effects of emerging technologies, he concluded in 2005 that "privacy as we define it will no longer exist".

8 The National Institute of Standards and Technology provides policymakers with regular reports on the performance of identification algorithms. As U.S. police officers have access to a photographic database covering the majority of the population, the potential of facial recognition is felt more distinctly there.

9 A May 2019 English poll on London police experiments indicated that barely 57% were in favor of using street-level facial recognition. This percentage rose to 83 when the purpose was to search for serious offenders. Acceptability among young people and minorities remains once again lower than the average for the population surveyed.

10 This principle, which is in keeping with European regulations (General Data Protection Regulation), was respected during the experimentation at the Nice Carnival in February 2019. In the United Kingdom, several lawsuits against the police are underway due to the lack of explicit consent of passers-by subjected to the recognition device.

11 This phenomenon is also amplified by the over-mediatization of these incidents, which have the dual appeal of the man-bites-dog piece of news and technological novelty.

The error rate must be guaranteed to be at an acceptable level, whatever the conditions of use (changing light, in motion, etc.)[12]. The quality of facial recognition software depends on its algorithm and the way it has been "trained". Analysis of the results of current systems has shown that the error rate is consistently higher for people of color and for women because white males are over-represented in the training sample[13]. The algorithm must work well to ensure that it is able to detect the right person at the right time. Thus, the way the algorithm works must be transparent and the conditions of its training scrupulously controlled with a baseline that meets verifiable qualitative criteria.

While there is little data on false negatives (non-detection of a target), the rate of false positives (detection of a target who is not one) is controversial for the same trials. For example, for its 2019 trials, the London police measured it at less than 1/1,000 (one error per 1,000 faces scanned) while researchers put it at more than 80% (the percentage of people wrongfully arrested following a match by the system)[14].
Finally, in order for the system to be relevant, its effectiveness must be maintained even in the event that a person attempts to conceal their face (by wearing a cap, glasses, a mask, hairpiece, scarf, or holding an umbrella). Otherwise, the target will use those countermeasures to fool the system, as was the case during the demonstrations in Hong Kong. This raises the question of prohibiting and penalizing the concealment of one's face on the public highway, which is difficult to implement.

The way the information system works must be protected against internal threats, as is the case for all police data processing, by imposing permanent traceability of operators' actions in order to avoid misuse and misappropriation.
With regard to external threats, it constitutes a choice target for hackers with libertarian or more basic material motivations, but also for the intelligence services of a third State for espionage purposes. Its architecture and infrastructure must be not only perfectly secure but also resilient. Operating parameters must be constantly monitored to detect any anomalies resulting from a hack. The advantage, in this respect, remains with the attacker.
Since biometric data is inherently sensitive, it must be protected against theft, its integrity must be guaranteed against modification or destruction, and its timely availability must be ensured for the system to function properly.

This prerequisite can only be achieved in a consolidated legal environment, whether for experimentation or operational implementation on the public highway.

III) The need: a consolidated legal framework with ethical and scientific monitoring

The French National Commission for Information Technology and Civil Liberties (CNIL) is regularly called upon to arbitrate on whether the uses of this technology is legitimate. Using the General Data Protection Regulation (GDPR) and the European "police-justice" directive as references[15], it examines on a case-by-case basis the grounds for exceptions to the legal prohibition of biometric data processing[16].
Aware of the multiplication of use cases, since September 2018 it has called for "a democratic debate...[and] asks the legislator to take up these issues "[17]. On June 21, 2019[18] the Minister of the Interior concurred, as did parliamentarians over the summer[19]. A collegiate and scientific reflection could usefully take place before the

12 Under perfectly controlled conditions (the PARAFE system – the French passport-verification program – used in airports), it is less than 0.5%.
13 https://www.lefigaro.fr/secteur/high-tech/amazon-somme-de-ne-plus-vendre-sa-technologie-de-reconnaissance-faciale-a-la-police-20190404
14 https://information.tv5monde.com/info/reconnaissance-faciale-nouvelles-polemiques-apres-l-echec-cuisant-de-la-police-de-londres
15 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016.
16 On July 17, 2019, la Quadrature du Net announced that it had filed a plea with the Conseil d'État, to overturn the decree authorizing the creation of the "Alicem" application (Certified Online Authentication on Mobile). Based on the opinion issued by the CNIL (National Commission for information technology and civil liberties), the association denounces the forced use of facial recognition in the application process. It considers that this approach does not comply with the principle of free consent provided by the RGPD and considers that it contributes to the trivialization of this technology.
17 https://www.cnil.fr/fr/la-cnil-appelle-la-tenue-dun-debat-democratique-sur-les-nouveaux-usages-des-cameras-video
18 https://www.lefigaro.fr/flash-actu/videosurveillance-castaner-veut-un-debat-sur-la-reconnaissance-faciale-20190621
19 Note 14 by L'office parlementaire d'évaluation des choix scientifiques et technologiques (Parliamentary office for the evaluation of scientific and technological choices)

legislative work, helping to guide the public debate, following the example of what is done regarding the issue of bioethics[20]. Respect for the principle of strict proportionality, long established in administrative law concerning infringements of individual freedoms (privacy, anonymity, freedom of movement, etc.), will form the basis of this reflection.

Internationally, the absence of any legal framework with regard to this technology is similar, and the level of litigation in each country depends on the extent to which populations are attached to their individual freedoms. For example, the United Kingdom, a leading European country in the deployment of facial recognition, is facing several lawsuits challenging the legal basis for its use on the public highway.
With a view to consolidating the security technology market, companies themselves are calling for some regulation, and sometimes taking sub-regulatory initiatives. *Microsoft* and *Google* have decided to respect principles of accountability in the development of artificial intelligence (AI) technologies and are suggesting that their competition do the same[21].

However, fear or the precautionary principle must not prevent experimentation, which is the only way to lay bare the biases as well as the benefits of an innovation. The development of a balanced regulation can only be achieved provided that some strategic management is put in place to avoid getting lost among myriads of initiatives. In all transparency, these tests in real-life situations must be scientifically assessed and their results shared publicly[22]. Within a sufficiently flexible legal framework, they would allow French manufacturers to develop sovereign solutions and no doubt allow for other approaches also based on video protection but perceived as less intrusive. For example, the Chinese company WATRIX is experimenting with a gait recognition software that would make it possible to identify a person from behind or hiding his or her face[23]. Scientific endorsement, the watchful control of a judge and of an independent administrative authority are all key elements to reassure the population. If, in addition, they perceive an objective gain in security and, above all, a reduction in constraints[24] (the famous improved user experience), this technology will be accepted.

In conclusion, it is clear that the political, legal and social systems are not ready to manage this technology, like all the other NBIC[25]-derived technologies. Facial recognition as a tool for administering populations needs to be part of a political project. In a democracy, it is imperative that the public debate establish the functional limits and acceptable use cases, while bearing in mind possible abuses, and not just the expected benefits. Research should therefore not be limited to the technical aspect but should be intensified in the fields of sociology and ethics in order to set the limits of use and to pave the way for acceptance. "We must put science back at the heart of public decision-making "[26].

Translated by SLT Max VRTOVSNIK and the French Gendarmerie Officers Academy Language Department

20 An initiative along this line was launched in June by the Conseil national du numérique (national digital council).
21 https://www.actualitesdudroit.fr/browse/affaires/immateriel/18182/reconnaissance-faciale-microsoft-devoile-six-principes-et-appelle-a-legiferer
22 The very positive experimentation report written by the municipality of Nice concerning the 2019 Carnival does not have the "scientific" qualities nor the "technical precision" expected by the CNIL (National Commission for information technology and civil liberties).
23 KANG, Dake, « Chinese 'gait recognition' tech Ids people by how they walk », *Associated Press* on : https://apnews.com/article/bf75dd1c26c947b7826d270a16e2658a
24 As was the case for the soccer world cup in Russia with Fan ID (free visa, fast access to the match and to public transport). The Rugby World Cup in 2023 and the Paris Olympics in 2024 represent remarkable opportunities to convince the population of the value of deploying facial recognition.
25 Nanotechnologies, Biotechnologies, Information technologies and Cognotechnologies (artificial intelligence).
26 Statement by the French Minister for Higher Education, Research and Innovation on September 2nd 2019.