WHITE PAPER FOR L'OBSERVATOIRE DE L'ÉTHIQUE PUBLIQUE

Crowd Surveillance

FOR A FRAMEWORK OF « PHYSIOGNOMONIC » AI

[OVERVIEW]

Région Hauts-de-France

OBSERVATOIRE DE L'ÉTHIQUE PUBLIQUE

C.Lequesne Roth & J.Keller

APRIL 2023

Caroline Lequesne – Roth

Maître de conférences HDR en Droit public à l'Université Côte d'Azur, membre du GREDEG (CNRS – UMR 7321)

Jonathan Keller

Ingénieur de recherche (Département SES, Institut Mines Telecom), chef de projet du Projet Living Lab 5G mené en partenariat avec la SNCF, Nokia et Orange et financé par la Banque Publique d'Investissement (BPI)

The regulation of identification technologies has been a topic of social and legal interest for over two years. From facial recognition to video surveillance, numerous reports and proposals have been produced in response to the European dynamic. It is important to emphasize that the legislator should and has to intervene for legal security and, more broadly, democracy. The juridical framing of ethical issues is also essential to prevent the instrumentalization of ethical charters and other "good practices". Recent history of technology has shown that such drifts can occur: technologies induce a bias of acceptability, which could lead to a loosening of regulatory constraints and ultimately institutionalize democratically contestable practices. The present study has drawn several conclusions:

- Physiognomical AI identification systems (facial, emotional, and behavioural recognition) have been the subject of numerous **scientific studies** and increasing **interest from law enforcement authorities.**
- At the same time, these systems continue to raise concerns among the public regarding their risks. The **risk of infringement of fundamental rights** is particularly high for individuals concerned: risks to privacy, freedom of expression, association, and movement. They are all the more significant as these systems process sensitive data - biometric data - which is immutable. Potential breaches of biometric data open the way to identity theft, which offers few solutions (unlike theft of access codes). These technologies also raise concerns in terms of **data security and sovereignty**.
- In terms of deployment, the industrial sector's offer does not meet the expectations of the public surveillance domain due to an uncertain legal and procedural framework. In addition to the lack of legal foundations, the analysis reveals that the **accountability regime** is not adapted to the identified risks.
- Although the current legislative proposals (namely, the European proposal for an Artificial Intelligence Act and the French Experimental Law for the 2024 Olympics) offer some initial solutions, they fail to address all the identified challenges:
  - The AIA provides a legal basis for the deployment of some surveillance technologies in publicly accessible spaces. However, the proposal refers the ball back to the legislators to develop the deployment procedures necessary to respect constitutional and conventional guarantees.
  - The Experimental Law lays the groundwork for these procedures for so-called intelligent video surveillance. However, it struggles to identify risks and does

not establish any substantial counter-power, which is concentrated in the hands of the executive.

These recommendations aim to enhance the legal framework and create stronger conditions for digital democracy.

1. *Strictly limit the use of physiognomonic AI*

Due to the risks associated with these technologies in terms of security and fundamental rights, particularly regarding mass surveillance, their use for law enforcement should be significantly restricted. We recommend that their prohibition for real-time identification purposes in publicly accessible spaces be strictly maintained, in line with Article 5 of the AIA. Furthermore, **the scope of any exceptions should be strictly limited and well-defined,** as the AIA appears overly broad in this regard, thus reducing the effectiveness of the prohibition.

Concerning facial recognition, the exceptions refer to the criminal offences outlined in Article 2(2) of Council Framework Decision 2002/584/JHA, which encompass economic offences, among others. These should be excluded and only pertain to crimes that endanger or violate **individuals' physical integrity.** Given the risks associated with the technology, the principle of **proportionality** requires that the use of facial recognition cannot be subject to any other alternative.

The distinctions between authentication and identification appear justified in light of the **risks** involved. Identification operations must be subject to stricter regulation.

The principle of proportionality requires **the prohibition** of facial recognition for identification purposes in certain areas, such as **schools, educational institutions, and workplaces.** Furthermore, adherence to the principles of proportionality and necessity demands that the use of technology must be **narrowly defined** (specifically in terms of duration and scope) and only employed in exceptional circumstances where the safety and well-being of individuals are at risk.

2. *Identify the competent authorities*

Identifying competent authorities and their resources is crucial to establishing an effective and enforceable accountability framework. The AIA has sparked a debate, already underway in the literature, regarding control authorities for intelligent systems. The proposal includes the establishment of dedicated national authorities within its governance model. Given the necessary coordination between the right to personal data protection and this emerging right, the **French Data Protection Authority** (Commission National Informatique et libertés - CNIL) appears to be the designated organization to manage accreditation and control responsibilities. The CNIL has expressed this opinion in a joint statement with its European counterparts. This proposal seems promising, provided the CNIL is **allocated additional financial, human, and technical resources** to fulfil its new responsibilities. Furthermore, joint controls between authorities should be raised and explicitly established, combining technical and legal controls.

Regarding the use of physiognomic technologies **by law enforcement**, it is essential to establish various controls based on two factors: the timing of deployment (authorization/post-use control) and the police powers in question (administrative/police powers).

In a preventive context **(administrative police),** authorization for deployment - which would involve exceptional surveillance of a publicly accessible space - could be granted by the **CNIL.** The CNIL would also ensure adherence to the defined protocol and conduct post-use controls. In this regard, it would be advisable to differentiate between agents (or even units) responsible for accreditation and those dedicated to post-use control.

In the context of repressive law enforcement activities **(judicial police),** following criminal procedure law, authorization should be granted by a **judicial judge.**

Moreover, it is crucial to update **the internal controls of agents** in response to the advancement of technological equipment used by law enforcement agencies. Beyond facial recognition technology, the adoption of artificial intelligence tools, such as predictive policing, calls for careful attention to the training of law enforcement agents, their authorization to use these technologies, and the supervision of their implementation. The legislature could demonstrate innovative thinking by utilizing existing structures to create **"Tech" units** within the Inspection

Générale de la Police Nationale (IGPN) and the Inspection Générale de la Gendarmerie Nationale (IGGN), comprising engineers and legal professionals who would oversee audit missions.

3. Authorize and control

To establish a sustainable framework, we propose implementing a "bicameral" prior authorization system based on the relevant police powers (administrative/judicial) and a post-use control regime that ensures compliance with usage guidelines.

Consistent with constitutional and European legal precedents, the deployment of physiognomonic technologies must be **limited** in scope:

- In a preventive context (real-time), it should be limited in time (to events presenting a risk to public order), in space (to a specific perimeter), and restricted to authorized personnel.
- In a repressive context (post-use recognition), it should only be allowed upon request to the judicial judge. We recommend treating facial recognition searches as **acts of information or instruction.**

In accordance with the principles of necessity and proportionality, as well as Article 5 of the AI Act, any authorization granted must be contingent upon the implementation of a dedicated protocol that outlines the guarantees adopted and adapted, including but not limited to:

- Public information dissemination;
- Data minimization (i.e. the data to be retained and the retention time);
- Human supervision (i.e. a system for verifying the results generated by the systems);
- Data security (commercial solutions such as Clearview are both illegal and technically risky);
- Data traceability;
- The procedures for evaluation and ex-post reporting requirements (e.g., technical errors and biases, as requested by the CNIL following the experiment conducted by the French city of Nice).

- The protocol must also specify the processing purposes, the system's deployment dates, and the authorized personnel to request queries.

The factors above are crucial given that the AI Act delegates regulatory authority to the private sector through a debatable certification system. Specifically, such organizations will be assigned to the compliance procedure for "high-risk" systems, including facial recognition systems, as stated in Article 43-1. These entities will be responsible for establishing the methodology and evaluation criteria. As a result, this model endows private actors with a significant role in regulating market access and ensuring compliance standards. Therefore, imposing protocols and audits specific to public administration is critical.

4. Recognize the normativity of digital acts

The normativity of digital practices and acts carried out by governmental bodies is currently disregarded, as highlighted by the Constitutional Council on June 12, 2018. Recognition of the normativity of searches conducted with these software programs is imperative. The control report issued by the Belgian Information Police Control Body reveals concerning practices that challenge the rule of law. Specifically, the report notes that facial recognition tools are used by the Belgian police force as if they were searching on an internet search engine[1]. These biometric processes frequently occur during the preliminary phase of an investigation and are not recorded or logged in any existing police databases. Consequently, these biometric processes are conducted outside the "legal radars" and democratic imperatives.

The use of facial recognition must be equated, within criminal procedures, to **acts of information or instruction** and subject to the same regulations.

5. Strengthening the duty of information

Law enforcement agencies should be subject to **an obligation to inform** the individuals concerned when they make use of these technologies. For this information duty to be effective, it should be multi-level and multi-media. During experiments conducted in public

[1] *Rapport DIO21006, Février 2022.*

spaces in the United Kingdom, non-governmental organizations highlighted that, despite the authorities' efforts, signage was insufficient to enable the individuals concerned to exercise their rights (or to consider alternatives when the experiments were based on consent) and to understand the issues. The Court of Appeal, which ruled on the use of facial recognition by the police in Wales, confirmed this analysis: the three-fold system deployed (information on social media, police vehicles, and flyer distribution) was insufficient to prevent violations of the right to privacy ([2020] EWCA Civ 1058 §20). The information duty should also be subject to a protocol (implemented by the supervisory authority or in collaboration with it during experiments). Failing this, there is a risk of "normalizing" this right, disregarding the social acceptability that it should promote.

6. Improving impact assessments

Our analysis has highlighted the shortcomings associated with impact assessments. They result from the absence of an express obligation and the discretionary nature of the method (the decision to conduct such assessments and the identification of risks are left to the sole discretion of the data controller).

To enhance transparency in the use of such technologies, **the legislator should require the publication of the data protection impact assessment (DPIA)** conducted before deploying any identification system in public spaces. To enable effective control, any user of such a system should submit their DPIA to the data protection authority (CNIL) before any deployment. At a minimum, the data controller should be required to publish a clear summary that is accessible to non-experts. This summary should include, in an intelligible form:

- All decisions or situations subject to automated processing,
- Criteria involved in decision-making,
- Information on data used,
- Description of the data collection method.

This summary could be purged of all technical elements (and focused solely on the type of data collected and their precise processing) to preserve trade secrets. The communication of DPIAs would provide both the concerned public and the CNIL with an additional means of control.

Additionally, we recommend making the legal consultation for physiognomonic AI users a paid service to allow the CNIL to acquire the necessary human and technical resources to carry out this control.

Finally, we urge the legislator to specify the methodology for AIPDs related to physiognomonic AI as follows:

- The analysis should mainly focus on the plausibility of risks by meeting safety, security, and robustness requirements from the design phase
- The examination should conduct an impact analysis to ensure that specific characteristics such as gender or skin colour are excluded to avoid illegal discrimination;
- The analysis should particularly identify potential negative impacts of the processing system on human rights by documenting all model developments;
- The analysis should be controlled, similar to what is done in the financial sector, by two competing private entities to ensure the sincerity of results;
- The analysis summary should be communicated in the Official Journal or an official municipal bulletin.

7. Question the consent regime.

There is a clear difference in acceptability and regime between individual uses of identification AI (such as unlocking smartphones and job interviews) and their use in places accessible to the public. This is due to the different purposes of the treatments (individual surveillance versus public surveillance), which entails **different legal basis.**

However, there is a collision between the two regimes: why is facial recognition technology acceptable for unlocking our phones but not for helping find a lost child or in some restrictive conditions?

Given the previously mentioned risks**, the consent regime** (which primarily characterizes private uses) must be challenged in some cases, such as in the workplace, to prevent unequal power dynamics and disproportionate use. At the same time, the public regime must be designed and built around restricted uses that provide strong guarantees in terms of control and accountability. Social acceptability will largely depend on these factors: transparency from authorities, information for the public, and established controls are essential in this regard.

CRÉDITS

Mise en page : Anaïs Rebuccini (Observatoire de l'éthique publique)

Images : sauf mention contraire, toutes les images utilisées dans ce document sont libres de droits et diffusées sous licence adobe stock

OBSERVATOIRE DE L'ÉTHIQUE PUBLIQUE

Région Hauts-de-France

WHITE PAPER FOR L'OBSERVATOIRE DE L'ÉTHIQUE PUBLIQUE

Crowd Surveillance

FOR A FRAMEWORK OF « PHYSIOGNOMONIC » AI

https://www.observatoireethiquepublique.com/
IEP de Lille – 9 Rue Auguste Angelliers – 59000 LILLE
E-mail : contact@observatoire-ethique-publique.com
Twitter : @ObservatoireEP
LinkendIn : L'Observatoire de l'Ethique Publique