European Review of Digital Administration & Law - Erdal
2021, Volume 2, Issue 2, pp. 205-210
ISSN 2724-5969 - ISBN 979-12-5994-752-9- DOI 9791259947529 17

*Law and "Smart Videoprotection": the French Case**

Sabrina Hammoudi
(Ph.D. Candidate in Public Law at University of Montpellier)

French Data Protection Authority, Opinion n. 2020-136 of 17 December 2020

Opinion on a draft decree about using "intelligent video" to measure the percentage of people wearing masks in transports. The draft decree allowing, over a one-year period and for statistical purposes, measurement by intelligent video devices of the rate of people wearing masks in public transports or public spaces assigned to such transports, has a determined, explicit, and legitimate purpose. The right for data subjects to object to such automatic processing can be excluded provided that they are informed about the exclusion.

ABSTRACT The french data protection authority (FDPA) delivered its opinion – requested by the Minister for transports – on the draft decree implementing the use of "smart video" techniques to measure the "mask wearing" percentage in public transports. This case is an opportunity for the FDPA to monitor compliance to the GDPR of such devices and raises important questions about new technologies legal framework in times of health emergency.

1. *Introduction*

Early on, humans learned the importance of quantifying the world: access to knowledge through numbers allowed them to better understand their environment and evolve in accordance with it, to adapt, survive and grow as a species. This will upon world's rationalization recently seems omnipresent[1], driven by the proliferation of "smart"[2] technologies and the possibilities they hold. Confronted with the present health situation, as it was already the case with terrorist acts[3], these technologies do not simply enable humans and institutions to obtain more knowledge but also to identify and protect themselves from defined dangers. We can therefore understand their proliferation, in France and Europe, in a political context embossed by the COVID-19 epidemic.

In this time of exacerbated health control, on 17 December 2020, the FDPA issued an opinion on the draft decree relating to "the use of smart video to measure the rate of people wearing a mask in transport". The publication took place in March 2021, at the same time as the publication of the decree. The decree of 10 March 2021[4] allows operators and managers of collective passenger transport services and spaces assigned to these services (railway stations for example) to use the "video protection"[5] systems authorized by the Internal Security Code[6] to measure the rate of people wearing a mask in these various places.

The video system in question "integrates a specific software processing allowing the real-time analysis of the video stream". It is also specified that the cameras are fixed, and that images are neither stored nor transmitted to third parties. In addition, these images are "instantly" transformed to be anonymized by blurring the people faces. A twenty-minute

* Article submitted to double-blind peer review.

[1] On this subject: A. Supiot, *La gouvernance par les nombres*, c*ours au Collège de France,* Paris, Fayard, 2015, 512; O. Rey, *Quand le monde s'est fait nombre*, Paris, Stock, 2016, 328.

[2] From Smartphone, to smart cities trough smart contracts and refrigerators, this adjective is now widely used. It seems relevant to note that this tendency is not new: N.D.R. Goddard, R.M.J. Kemp and R. Lane, *An overview of smart technology*, in *Packaging Technology & Science*, vol. 10, issue 3, 1997, 129-143.

[3] On this matter: Q. Eijkman, *Counter-Terrorism, Technology and Transparency: Reconsidering State Accountability*, in *The International Centre for Counter-Terrorism – The Hague* 3, n. 1, 2012.

[4] Decree n. 2021-269 on the use of smart video to measure the rate of people wearing a mask in transport, March 10 2021.

[5] Recent distinction, in French, between "video protection" and "video surveillance"; According to the FDPA website, video protection devices film "publics roads and public places: street, station, shopping center, shopping area, swimming pool etc.", video surveillance devices film private places which are not open to the public: store's reserve, warehouses, closed condominium etc.

[6] Internal security code, article L. 252-1.

actualization is implemented to assure that no one could be geolocated. The decree also explicitly provides for the non-application of the rights of access, rectify, erase and object to the automatic processing, as formulated by GDPR third section.

The FDPA, referring to Data Protection Act article 8[7], had issued a positive opinion to the draft decree, subject to certain information that were added to the final decree writing. Several issues punctuate the authority's reasoning: is it a question of biometric data? Is the draft decree GDPR compliant? More broadly, this seemingly anecdotal case leads us to reflect on the legal status of smart video devices and highlights the shortcomings of a regime that still deserves to be improved.

2. *Absence of biometric data processing*

First, the FDPA begins by clearly stating that the video device in question is not "intended to process biometric data". By doing so, the authority expressly clarifies that the data in question cannot be included in the qualification of "sensitive data" and thus do not comply with the stricter regime of GDPR article 9. It "takes note that the purpose of these device is not and cannot technically be, to identify individuals and is, therefore, not intended to process biometric data". This functional reasoning is fully consistent with the definition of biometric data as recognized by the GDPR. In the present case, since the purpose is to identify the data subject, it is then possible to assert that the data in question is not biometric, especially since faces are instantly anonymized by the software. This solution is therefore not surprising and the GDPR itself states that "the processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person".

It is interesting to note that the regime applicable to sensitive data, referred to in GDPR article 9, is certainly stricter than the general regime applicable to personal data, but it nevertheless has an exception that could have been accepted in the present case if the biometric data qualification have been deemed relevant: the collection of biometric data is possible if there is a "superior public interest" justifying it[8], however, that overriding interest is very close to that accepted by the FDPA, in the second part of its reasoning, and which will justify excluding the right of opposition of the persons concerned[9]. Thus, one can legitimately think that the FDPA would have approved the processing, even in the presence of biometric data.

The FDPA's clarification about the "non-biometric" nature of the processed data has therefore little practical impact but is theoretically important: this case is an opportunity to highlight, as the FDPA had already done in the past, the existence of intelligent video systems potentially infringing on rights, without being facial recognition systems.

Many systems, although based on video technologies, do not aim to recognize the data subjects (as in traditional video protection and facial recognition) but simply to detect risky situations. As Winston Maxwell points out: "Powered by CCTV footage, a system can generate an alert if it sees an inanimate body on the sidewalk, a road accident, a crowd movement, a fire. These systems aim to identify a situation, not a person. But they can be diverted from their original purpose and become tools for widespread surveillance [...]"[10].

[7] Data Protection Act, Law n. 78-17, 6 January 1978, relative à *l'informatique, aux fichiers et aux liberté*, article 8-4: "(The FDPA) keeps abreast of the evolution of information technologies and makes public, if necessary, its assessment of the consequences resulting from it for the exercise of the rights and freedoms […] As such, it shall be consulted on any draft law or decree […] relating to the protection of personal data or the processing of such data".

[8] GDPR, article 9-2, biometric data collection is possible if it "is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject".

[9] GDPR, article 23: "Union or Member State law to which the data controller or processor is subject may restrict by Way of a legislative measure the scope of the obligations and rights […] when such a restriction respects the essence of the fundamental rights and freedoms and is has necessary and proportionate measure in a democratic society to safeguard [...] other important objectives of general public interest of the Union or of a Member State, in particular year important economic or financial interest of the Union or of a Member State, including [...] public health and social security".

[10] W. Maxwell. *Vidéo intelligente dans les trains, bus et*

The start-up company behind the device in question has also set up another similar system: an algorithm designed to streamline border crossings[11]. This device, capable of determining the number of people in a checkpoint, if those people are wearing glasses or not, the position of their face, etc. works in conjunction with other carried out biometric border identity control technology. Quite interestingly, the algorithm does not itself control the identity, and therefore would not be, according to the before mentioned reasoning of the FDPA, a processing of biometric data, but it interacts very closely with biometric technologies.

The spectrum is therefore wide, from conventional video protection technologies, whose legal regime is clearly defined to facial recognition technologies that have already been banned by the domestic judge[12], through intelligent video device that detects personal data other than the picture of the data subject[13], those automatic process are to blur the definition of personal data even further.[14]

Acknowledging that the video device in question is not a processing of biometric data, but implicitly admitting that this is indeed a processing of personal data, the FDPA analyses the decree's compliance to the GDPR.

3. *A GDPR compliant device*

The FDPA legal reasoning is divided into two parts: first, the question is one of verifying the conformity of the device's "purpose", according to GDPR's article 5. Then, the FDPA analyzes the exclusion of opposition implemented by the decree, according to GDPR's article 23.

According to GDPR, article 5.1.b, personal data must be, among other things, "collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes". In the present case, the authority acknowledges that the treatment "is not intended to prosecute violations of the regulations relating to masks" or even to allow "the immediate deployment" of repressing public officials enforcing these regulations, but rather has a simple educational purpose[15]. The goal is then to "broadcast typical and non-targeted advertising messages" and to deploy "informational public officials to increase users' awareness of their obligations".

The FDPA thus considers without further details that the purpose of the processing is determined, explicit and legitimate. One may wonder why the last article 5.1.b criterion - the prohibition to further process in a manner that is incompatible with the first proposes - is not investigated. The most obvious answer seems to be the following: since photographic data is not stored, the question does not seem to arise, technically, for the FDPA.

In a second step, the FDPA analyses the decree's exclusion of the right to object for data subjects. GDPR article 23 makes it possible to limit the rights of data subjects to preserve "important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including [...] public health and social security"[16].

The FDPA notes above all the "unprecedented" nature of this exclusion and the link between wearing masks and the fight

métros : attention à l'effet "cliquet", entretien de Winston Maxwell, Recueil Dalloz, Paris, Dalloz, 2021, 692.

[11] D. Licata Caruso, *How artificial intelligence will streamline border crossings at train stations and airports*, in *Le Parisien,* 14 October 2021.

[12] The French administrative judge has banned the experimentation of facial recognition in high schools: Administrative Court of Marseille, 27 February 2020, n. 1901249; C. Crichton, *Annulation d'un dispositif expérimental de reconnaissance faciale dans deux lycées*, Dalloz Actualité, March 10 2020.

[13] The French High Administrative Court and the FDPA has recognized the personal nature of data processed by thermal cameras: Council of State, ord. 26 June 2020, n. 441065; M.-C. de Montecler, *Quand l'utilisation des caméras thermiques est-elle soumise au RGPD ? Actualité juridique du droit administratif* (AJDA), Dalloz, 2020, 1319; FDPA, *Caméras dites "intelligentes" et caméras thermiques : les points de vigilance de la CNIL et les règles à respecter,* June 17 2020.

[14] Beyond this particular case, on the blurred definition of personal data/public data J.B. Auby in J.B. Auby, V. De Gregorio, *Données urbaines et smart cities*, Boulogne-Billancourt, Berger Levrault, 2017, 198.

[15] If the device's purpose had not been simply educational, it would entered the legal regime of the "police justice" directive: (EU) 2016/680, 27 April 2016, on protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.

[16] It should be noted that the FDPA cites this article by mentioning only public health and not the economic imperative in which it is understood in the original GDPR writing.

against COVID-19. It then considers "that these devices pursue public health objectives and protection of people allowing to consider a limitation of their rights". After finding that the exclusion of rights was justified, the FDPA verifies whether the draft decree complies with the minimum "specific provisions" listed in article 23.2 GDPR. At the end of its analysis, the Commission expresses two reservations, which will be respected in the decree's final writing: on the one hand, the draft decree did not explain clearly enough that the video devices were based on algorithmic processing, nor did it mention the right of data subjects to be informed of their rights limitation. The 10 March 2021 decree, having taken into account these two recommendations, therefore appears to comply with the GDPR in the eyes of the FDPA.

It should be noted that the control operated by the FDPA is based on two main concepts, both linked to each other and frequently used in new-technologies regulation: information and transparency. These two principles are relevant in personal data law and algorithm law, whether at the French or European level[17]. Also, as Professor Auby points out, "The constant increase in the transparency of public data is very important, especially as it tends to restore a sort of balance of powers between citizens and public authorities: the more citizens have access to data on the functioning of public institutions, the more they can assess their policies, propose new policies and draw conclusions for subsequent elections [...] However, we must not exaggerate the scope of this. The issue of the digital divide remains central, but in addition to the fact that access to public information benefits, at least until now, only a minority of people - who have the ability to master electronic and digital tools that predominantly have an academic background or associative experience - should not be forgotten that the digital revolution also brings its own opacity, as noted about algorithmic governance"[18]. While the present case does not aim at the communication of an incomprehensible source code, it nevertheless illustrates the limits of transparency and the right to information. In our case, these principles lead specifically to informing the data subjects that they are subject to automatic data processing, but that they cannot exercise any rights over it. Such a mention was essential and the exclusion of right must, of course, be notified. However, can we really think that, faced with such a mention, the citizen feels empowered? He knows he is being filmed, he knows he is being "counted" and, although reassured about the fate of his personal data in the short term because of the strong guarantees provided by the process, he nevertheless remains the subject of a form of opaque algorithmic governance whose concrete effects he does not yet measure.

In addition, it is important to note that the commented devices had already been put in place, in Cannes as well as in a large Paris metro station in May 2020, nearly a year before the publication of the decree: it was then possible, for data subjects, to express their consent or lack of consent by a head gesture. These experimentations were aborted following a FDPA publication, in June 2020, which stated that the right to object was not sufficiently ensured: "The devices brought to the attention of the FDPA which provide for the possibility for people to manifest their opposition by a significant body movement, such as a head 'no', do not appear satisfactory from the individual's protection point of view. This solution is impractical and difficult to generalize. It also forces individuals to publicly display their opposition to the treatment and puts too much of a burden on the person, especially if that kind of device multiplies. In principle, such modalities do not ensure the effectiveness of the right to object and must therefore be considered as non-compliant with the GDPR". The Autonomous Parisian Transportation Administration then decided to stop the experimentation in order to "complete the device of right of opposition as requested by the FDPA". It finally did not have to do so thanks to the March 10 decree which, falling under the qualification of "law" within the meaning of article 23 GDPR, made it possible to exclude the right to object. This reasoning, legally valid, must be considered from the citizens point of view who, not perceiving the GDPR normative "finesse" may simply feel dispossessed of a right so

[17] On the legal existence of transparency, including in France: A.G. Orofino, *The Implementation of the Transparency Principle in the Development of Electronic Administration*, in *European Review of Digital Administration & Law*, vol. 1, issue. 1-2, 2020, 123-142.

[18] J.-B. Auby, *Administrative Law Facing Digital Challenges*, in *European Review of Digital Administration & Law*, 2020, vol. 1, issue 1-2, 7-16.

important that its protection was supposed to be improved.

4. *Outstanding questions on proportionality*

4.1. *The necessary determination of the device's effectiveness*

As the FDPA stated in its introduction, infringements of private life must not only be justified by public interest but also "necessary and proportionate to the public interest protection goal". The proportionality test is an important tool in the judge's hand when he balances public interest and individual freedoms. In the present case, the authority acknowledges that the commented system, even if it is limited to health emergency situations, presents an important risk: "generalizing a feeling of surveillance among citizens, creating an habituation phenomenon, trivialization of intrusive technologies and, ultimately, generating increased surveillance". Despite this global risk recognition, the FDPA does not analyses the device's efficacity, however a crucial element of the proportionality check. The FDPA only requests an a posteriori evaluation so that "the impact of such devices on the overall health strategy is evaluated and documented on a regular basis, so that their effectiveness and relevance over time can be evaluated". Yet, in this case, the device's efficiency is not evident: as Professor Netter points out: "Who can seriously say, after a year in which the pandemic has occupied the news from morning to night, that there are still citizens who ignore the usefulness of masks? Non-wearing or incorrect wearing are, obviously, fully conscious. Therefore, the only way for the device to have any practical interest it if it is misunderstood by travelers, wrongly fearing a sanction and correcting their behavior accordingly"[19].

The FDPA has already called for further monitoring about the effectiveness of such devices. A parallel can then be drawn with another FDPA's opinion about the global security act[20] in which, on the subject of insecurity preventing technologies, it regretted "that the effectiveness of these systems with regard to the legitimate objectives of public order and security has never been rigorously evaluated in a global way, and therefore considers that an independent evaluation mechanism of the relevance and effectiveness of these systems is more necessary than ever, given the risks for individual freedoms"[21].

While it can be argued that health emergency justifies deploying such a device without proving, upstream, its real effectiveness, it nevertheless seems essential that effectiveness should be sought by an impact study a posteriori. To our knowledge, this study has still not been carried out for the commented device whose implementation will stop next March, unless renewed by another decree.

4.2. *Immediate individual risk vs collective long-term risk*

Such cases, which may seem anecdotal, do not present strong individual risks because of the "privacy by design"[22] guarantees the tool provides. However, as Professor Netter points out: "In this case, it has been shown that the treatment is low risk from an individual point of view, but dangerous collectively, in that it contributes population acclimatization to public algorithmic surveillance. However, in front of these risks, the usefulness appears very low"[23].

The "collective risk" notion echoes that of "ratchet effect"[24]. As Professor Maxwell explains: "Those technologies most troubling aspect is the 'ratchet' effect. Each measure

[19] E. Netter, *"Vidéo intelligente" et port du masque dans les transports : la nécessité du malentendu,* in *Dalloz IP/IT*, 2021, 415.

[20] Global security act n. 2021-646, 25 May 2021, pour une sécurité globale préservant les libertés.

[21] FDPA, Deliberation n. 2021-011, 26 January 2020, opinion on a draft law on global security.

[22] For a definition and critical analysis of this notion: B.J. Koops and R.E. Leenes, *Privacy Regulation Cannot Be Hardcoded. A Critical Comment on the "Privacy by Design" Provision in Data-Protection Law*, in *International Review of Law, Computers & Technology*, vol. 28, issue 2, 2014, 159.

[23] E. Netter, "*Vidéo intelligente" et port du masque dans les transports : la nécessité du malentendu*, 415.

[24] This notion, developed in economic science, is recognized in regulation process: V. Bhaskar, *The Ratchet Effect Re-examined: A Learning Perspective*, in www.cepr.org, 2014; M.A. Meyer, J. Vickers, *Performance Comparisons and Dynamic Incentives*, in *Journal of Political Economy*, vol. 105, issue 3, 1997, 547, dx.doi.org/10.1086/262082. More recently, it is used in administrative science and public law in connection with the health crisis. See, among others: D. Schoenher, *Les libertés, victimes collatérales du Covid-19 ?*, Les Notes du CREOGN, Centre de Recherche de l'Ecole des Officiers de la Gendarmerie Nationale, 2020, n. 49; W. Maxwell, *Vidéo intelligente dans les trains, bus et métros : attention à l'effet "cliquet ", entretien de Winston Maxwell*, Recueil Dalloz, Paris, Dalloz, 2021, 692.

taken individually can probably be justified in the light of the proportionality test: legitimate objective, necessity of the measure, proportionality, clear and precise legislative framework. On the other hand, the cumulative effect of these devices is still poorly understood and constitutes a major societal debate"[25].

Beyond the FDPA's reasoning, this case demonstrates how difficult it is to relevantly regulate, smart video devices. It is important to realize that this device is not only a temporary private data-collection tool with strong privacy guarantees, but also a "reading tool", in administration's hand[26] aimed at conducting its public services missions and, eventually, helping its decision-making process. The relevant data in the commented case are not only video collected pictures, but also the data those pictures gave birth to numbers, percentages, that will be stored and used by the administration. It is then no longer only a matter of privacy protection, but a broader questioning about what is commonly named "algorithmic governmentality". Behind this tool are the potential discrimination risks, now widely known, of such process[27].

Faced with the proliferation of video devices based on personal data, but not intended to identify them, privacy should not appear as the only "gateway" to a juridical debate. In the commented case and similar ones, the FDPA[28] takes out the best of the means at her disposal but hope itself for the establishment of a large-scale regulation addressing the issue of these new technologies from a broader legal angle.

[25] W. Maxwell, *Vidéo intelligente dans les trains, bus et métros*, 692.

[26] Let us mention here how the notion of administration meets that of private corporation in such cases where the technology is developed and managed by a start-up company.

[27] On this subject, among a large variety of studies on indirect bias and algorithms, see: Council of Europe, *Discrimination, artificial intelligence and algorithmic decisions*, 2018.

[28] Let us recall in this respect that the FDPA, founded in 1978, remains an authority whose expertise is mainly focused on privacy.