apdcat
Autoritat Catalana de Protecció de Dades

Opinion in relation to the consultation regarding the Opinion issued by this Authority on the placement of cameras in access control and the use of these images for statistical purposes .

A query is submitted to the Catalan Data Protection Authority in relation to the Opinion issued by this Authority on the placement of access control cameras and the use of these images for statistical purposes.

In the consultation initially submitted, it was proposed that:

"(...) is interested in setting up a data collection and analysis system in the centers and facilities managed by society.
The type of data to be collected and exploited are in reference to the vehicles that access (number of vehicles, typology - trucks, trailers, vans -, routines when on routes and waiting times, ...) The planned technology foresees that the data collection is done through the analysis of images captured through the placement of cameras in the access controls to the different facilities, focused on public roads.
We ask the Agency to comment on this matter, on whether cameras can be placed, the images collected can be processed to obtain the indicated data, and whether this information can be transferred to a third party for exploitation and analysis. It is for the company's internal use and always for statistical purposes."

In the new document presented, it is stated that they have asked an independent firm to prepare an AIPD, which they attach so that the APDCAT can complete the Opinion issued.

Having analyzed the consultation, given the current applicable regulations, and in accordance with the report of the Legal Counsel, I issue the following opinion:

I

(...)

II

The considerations made in the aforementioned Opinion in relation to the legal nature of the applicant and with respect to the control of compliance with the data protection regulations corresponding to the Catalan Data Protection Authority (article 3.e) Law 32/2010) regarding the data processing carried out by it.

The Opinion, in relation to the query made, regarding the placement of access control cameras and the use of these images for statistical purposes, concluded that, with the information available, the company did not would be legitimate to install the intended video surveillance system given that it involved the capture of images from the public road.

Likewise, it was indicated that *"in the event that the capture of images is limited inside the facilities it manages, in order to be able to evaluate the legal adequacy of the treatment, this Authority should have a Memorandum, in terms of article 10 of Instruction 1/2009, where the characteristics of the treatment that you want to carry out are described in detail, the necessary weighting is done for the purposes of being able to apply the legal authorization based on the legitimate interest (art. 6.1.f) RGPD) and that allows to evaluate the proportionality of the data being processed and the scope of the treatments that are intended to be carried out, apart from the other extremes required by article 10 of the Instruction 1/2009 ".*

It should be pointed out that the conclusions of that opinion were not intended to require the presentation of new documentation, but that it was made clear that the information provided was insufficient to assess the adequacy of the treatment. In any case, in accordance with the principle of proactive responsibility (article 5.2 RGPD), it is the responsibility of the person responsible for the treatment to carry out a risk analysis and, to the extent that the treatment is for video surveillance, the preparation of a Report in accordance with what is established by Instruction 1/2009, of February 10, on the processing of personal data using cameras for video surveillance purposes, in everything that is not opposed to the RGPD, which describes in detail the characteristics of the processing to be carried out, or in its case a data protection impact assessment, if the result of the risk analysis shows its need.

As this Authority has previously highlighted, it will not be necessary to carry out the Report provided for in article 10 of Instruction 1/2009 when a data protection impact assessment (AIPD) is carried out, with the understanding that its content must be included in the aforementioned AIPD.

III

The entity has sent this Authority the Privacy Impact Assessment it has drawn up.

It is necessary to start from the premise that the final result of an impact assessment is a report, or a set of documentation, that collects the characteristics of the evaluated treatment and the decisions taken to mitigate its risks, in accordance with its identification, analysis and assessment. Based on these risks, the necessity and proportionality of treatment operations must also be assessed.

The RGPD sets in article 35.7 as the minimum content for an AIPD: the description of the processing operations, the assessment of the necessity and proportionality of the treatment, the assessment of the risk to rights and freedoms of people, and the measures taken to mitigate the risks.

In the case of data processing by video surveillance systems, Instruction 1/2009, of February 10, on the processing of personal data by means of video surveillance cameras also applies, in everything that is not opposed to the GDPR Article 10 of the Instruction provides that the Report must identify and describe the following issues:

"a) Organ, body or entity responsible: specification of the person responsible of the file, of the people operating the video surveillance system, as well, yes where applicable, of the person responsible for the installation and its maintenance.

b) Justification of the legitimacy of the capture and subsequent treatments that are foreseen: (...)

c) Justification of the purpose and proportionality of the system, in accordance with the which establish articles 6 and 7 of this Instruction.

d) Personal data processed: it is necessary to specify whether the voice will also be recorded and whether the purpose involves, predictably, the capture of images that reveal personal data specially protected or others that require a medium or high level of security.

*e) **Location and field of view of the cameras: reference must be made to the location and orientation of the cameras** . In particular, when it comes to cameras outside, it must be stated whether within a radius of 50 meters there are health centers, religious centers, places of worship or headquarters of political parties or educational centers attended by minors. It is also necessary to refer to the spaces that enter the field of vision of the cameras.*

*f) **Definition of system characteristics** . In this section you must specify:*

Total number of cameras that make up the system.
***Technical conditions of the cameras and other elements** .*
If the cameras have slots or connections for external storage devices.
If the cameras are fixed or mobile.
If images are captured on a fixed or moving plane.
If you have the possibility to obtain close-ups at the time of capture or once the images are recorded.
Whether the images are viewed directly or only recorded, with limited access to certain cases provided for in the Report.
If the capture, and if applicable the recording, is done continuously or discontinuously.
If the images are transmitted.
Forecasts relating to the mechanisms of identification and dissociation to attend the exercise of rights of access, rectification, cancellation and opposition.
When recording voice, you also need to specify the distance at which it can be recorded.

*g) Duty of information: **a reference to the number and location must be included information posters, as well as other additional means of information, in order to certify compliance with the duty of information** .*

h) Period for which the system is installed and period of conservation of the images.

i) Measures planned to evaluate the results of the operation of the system and the need for maintenance.

j) Security measures: specification of the level of security required and description

of the security measures applied.

10.2 The information referred to in sections e) and ig) must be accompanied of the corresponding graphic information.
(...)".

Therefore, the AIPD of a video surveillance treatment activity is also subject to the provisions of Instruction 1/2010 and, specifically, to what is provided for in article 10 of the Instruction, in this sense it would be appropriate that within the AIPD included all the issues referred to in the instruction.

From the analysis of the AIPD presented, it has been detected, on the one hand, that it does not contain information on some of the sections of article 10 of Instruction 1/2010. Thus, to give an example, information is missing on the following aspects:

- section e) relating to the location and field of view of the cameras.
- section f) regarding the definition of the system's characteristics with indication, among other aspects, of the total number of cameras and their technical conditions, the specification of the technology they incorporate, etc.
- section g) which requires identifying the number and location of the information posters to make effective the right of information of the interested parties.

This information is essential in the case at hand since, as indicated in the referred opinion, the capture of images of the public road is reserved for the security forces and bodies for the purposes provided for in Organic Law 7 /2021, of 26 May, on the protection of personal data processed for the purposes of prevention, detection, investigation and prosecution of criminal offenses and execution of criminal sanctions. In the event that this capture of the public road was only incidental, this situation would have to be duly justified to the AIPD itself.

On the other hand, some inconsistencies are detected in the AIPD's risk analysis. Thus, for example, in the section on " *Legitimation of treatment"* it is identified as a threat: *"when the treatment is based on the consent of the interested party, this is not granted freely, specifically, informed and/ or unequivocal or by means of a statement or a clear affirmative action".* And as justification for this threat the following is indicated *: "Consent is granted freely, specifically informed and unequivocal".* The following is indicated as a threat: *"In the case that the treatment is based on the legitimate interest, the interests of the subjects of the treatment are superior to those of the person responsible",* and " *"In the case that the treatment is based on the 'legitimate interest, the interested parties are not given an option to oppose this purpose' and,* as justification: *'The treatment is not based on legitimate interest'.* These statements are inconsistent with what is included on page 7 of the AIPD, which indicates that the legitimizing basis of the treatment is the legitimate interest of the entity.

Also in the risk analysis, in its *"Principles of Treatment" section* , it is identified as a threat: *"The treatment is incompatible with the purpose for which the personal data were initially collected"* and as justification " *The treatment is compatible with the original purposes".* However, this measure would make sense if the data being processed had previously been collected for a legitimate purpose and wanted to be used for a new purpose, but with the information provided it does not appear that this is a new use of a information available.

Another issue that does not seem well resolved by the AIPD, we find it in the Transfers section in which it is identified as a threat that *"Data communications occur outside the requirements of Article 6 RGPD"* and as justification: *"Data communications are in accordance with article 6"* . However, no section of the AIPD indicates that the data subject to treatment can be communicated or the legal basis that would underpin this communication.

In short, from the analysis carried out of the AIPD sent it can be concluded that it should be revised in order to include the information provided for in article 10 of Instruction 1/2009, of February 10, on the treatment of personal data through cameras for video surveillance purposes, as well as the rest of the requirements established by article 35.7 of the RGPD, in order to determine if there is a legal basis that enables it and if the rest of the principles and guarantees are met established by the data protection regulations.

IV

Finally, it should be remembered that article 36 of the RGPD establishes:

"1. The person in charge will consult the control authority before proceeding with the treatment when a data protection impact assessment under article 35 shows that the treatment _ _ ***it would entail a high risk if the person in charge does not take measures to stop it mitigate it***

2. When the control authority considers that the treatment provided that section 1 refers to could infringe this Regulation, in particular when the person in charge is not present identified or mitigated sufficiently the risk , the control authority must , within a period of eight weeks from the request for consultation, advise in writing to the person in charge, and in his case to the person in charge , and he will be able to to use any of them powers mentioned in article 58.
I say period will be able extend six weeks , depending on the complexity of the treatment expected _ The control authority will inform the person in charge and, where applicable , the person in charge of such an extension within one month of receiving the consultation request , indicating the reasons for the delay . These deadlines they can suspend until the control authority has obtained the information requested for the purposes of the consultation.

3. When consult the control authority in accordance with section 1, the person responsible for the treatment the will provide the information next :

a) if applicable , the responsibilities respective of the manager, the co-responsibles and the managers involved in the treatment , in particular in case of treatment within a business group ;

b) the ends and means of the treatment expected ;

c) measures and guarantees established to protect the rights and freedoms of the interested parties in accordance with this Regulation;

d) if applicable , the contact details of the data protection officer ;

e) the impact assessment related to data protection established in article 35, y

f) any another information requested by the control authority .

(...)"

According to this article, prior consultation with the Control Authority is only mandatory when the AIPD shows that the treatment involves a high risk if the person responsible for the treatment does not take measures to mitigate it.

As established in Article 36 of the RGPD, once the control authority has all the necessary documentation, it must respond in writing within eight weeks. This period can be extended by another six weeks, according to the complexity of the treatment.

In the context of a prior consultation, the data protection authority can use any of the powers contained in article 58 of the RGPD, both investigative and corrective, as for example *"to impose a temporary or definitive limitation of the treatment, including the prohibition"* .

In the case of the AIPD presented, it qualifies the inherent risk and the residual risk as bearable. In fact, it states in its conclusions: *"After the analysis of the characteristics of the treatment and the subsequent determination of the potential risks derived from it for the data protection right of those affected, it is concluded that the data processing derived from the processes of the cameras for statistical purposes, do not pose a risk that requires the prior authorization of the Control Authority to continue the treatment or that cannot be assumed".*

In the event that the revision of the AIPD in the terms contained in the legal basis III of this opinion, determines the legality of the treatment and, in its case, the risk rating varies, it should be remembered that the APDCAT provides of a specific procedure (accessible from its website www.apdcat.cat) so that those responsible for the treatment of their scope of action can request the prior consultation referred to in article 36 of the RGPD. To request this procedure, it is necessary to provide all the documentation provided for in paragraph 3 of the aforementioned article 36.

conclusion

The data controller should review the AIPD carried out in order to ensure that it includes both the information provided for in article 10 of Instruction 1/2009, of February 10, on the processing of personal data through cameras with video surveillance purposes , as well as the rest of the requirements established by article 35.7 of the RGPD.

consultation with this Authority is only mandatory when the AIPD shows that the treatment entails a high risk if the person responsible for the treatment does not take measures to mitigate it.

Barcelona, June 20, 2023