apdcat
Autoritat Catalana de Protecció de Dades

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

File identification

Dismissal resolution of sanctioning procedure no. PS 10/2020, referring to the Public Security Institute of Catalonia.

Background

1. On 02/15/2019, the Catalan Data Protection Authority received a letter from a person who filed a complaint against the Public Security Institute of Catalonia (hereafter, ISPC) on the grounds of an alleged breach of the regulations on the protection of personal data. Specifically, the complainant, an officer of the Local Police of the City Council of (...), reported the following:

- Unjustified access to your ISPC personal file. The reporting person claimed that an *"agent of the body (...) of police officers"* and a *"sub-inspector of the body (...)"* of the ISCP, in the month of January/(...) of 2019 , they made certain comments about him, referring to some data (which he detailed in his letter) that, according to the complainant, they could only have known by accessing his file.
- Disclosure of data relating to your person. The complainant stated that on the 4th or 5th of (...) 2019, the aforementioned sub-inspector (...) called the head of the Local Police of (...), facilitating this sub-inspector in the course of the conversation details about him, such as the fact that he was going to study in the ISPC library and the time he spent there. In this sense, the complainant transcribed in his written complaint an email that the head of the Local Police would have sent him, in which his superior referred to the conversation he had had with the sub-inspector of the PG-ME, in the following terms *"at all times he was cordial and respectful towards you, and about the strangeness of the time you were in the library, according to him important and possibly not compatible with the service in turn of the local police (...)"* .

2. The Authority opened a preliminary information phase (no. IP 50/2019), in accordance with the provisions of article 7 of Decree 278/1993, of November 9, on the sanctioning procedure of application to the areas of competence of the Generalitat, and article 55.2 of Law 39/2015, of October 1, on the common administrative procedure of public administrations (henceforth, LPAC), to determine whether the facts they were likely to motivate the initiation of a sanctioning procedure, the identification of the person or persons who could be responsible and the relevant circumstances involved.

3. In this information phase, on 03/19/2019 the reported entity was required to report on the following:

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

- Provide the log of accesses to the ISPC file relating to the person reporting here from 01/12/2018 to 15/02/2019 -both included-. It is necessary to justify each of the accesses to said file.

- Inform if the ISPC has any register containing data on the people who go to the library - as would be the case of the person making the complaint here - and the time they stay there.

- Report on the reasons that would have justified the call that the sub-inspector (...) made on the 4th or 5th of (...) 2019 to the local police chief of (...), and the legal basis which would justify the need to provide data relating to the complainant here (such as the fact that he was going to study in the ISPC library and the hours he spent there).

4. On 29/03/2019, the ISPC responded to the aforementioned request through a letter in which it set out the following:

- That *"there is no record of access to the generic part (data associated with the person) of the ISPC application, which is why no evidence can be provided".*
- That *"the Institute of Public Security of Catalonia does not have any register containing the data of the people who come to its library (Security Knowledge Center) and the time they stay there".*

- That *"the reason for the sub-inspector's call (...) to the local police chief of (...) is because of the continued presence and unusual behavior of Mr. (...), at the Security Knowledge Center of the Public Security Institute of Catalonia, based on the identification of the persons provided for in article 16 of Organic Law 4/2015, of March 30, of protection of public safety".*

The reported entity attached the following documentation to the letter:

- *"Informative note"* issued on 03/20/2019 by (...) (...), which sets out the following:
  "ISPC is a security site and, as such, it must follow the security measures and specific actions that the PG-ME has in the Specific Operational Plan (POE) with the current level 4 Anti-Terrorist Alert . (...) in order to be able to access the Security Knowledge Center and, consequently, the premises of the ISPC, Mr. (...) had to identify himself as an officer of the Local Police of (. ..). So, in order to comply with the provisions of the ISPC internal regulations and the POE, Mr. (...) identified himself to the ISPC Surveillance Unit as an agent of the Local Police of (...), without having to access any files. Therefore, no inquiry was made containing data from his personal file, simply, Mr. (...) provided the information that he was an officer of the Local Police of (...) in order to gain access to the premises.

  Along these lines, inform that there is no record that contains data on the people who go to the library and, even less, the time they stay inside".
- Report issued on 03/21/2019 by the sub-inspector (...), which includes the following verbatim:
  "Knowing that Mr. (...) a few days ago (on November 30, 2018) she had behaved inappropriately with the Chief (...) and that (...) she was a little afraid of a

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

presence and behavior of this user I decided to hold an interview with this gentleman in the company of the Chief (...).(...). Given the strange and inconsistent behavior of Mr. (...), together with the fact that his attendance at the CCS was continuous from morning to afternoon from Monday to Friday, which could be contradictory to the usual shifts of an agent of the police, I decided, for security reasons, to be able to check if this gentleman was really a policeman and was working as he said at the Local Police of (...). We cannot ignore that he used a police credential from this police force to access the CCS on a daily basis. I raised the desire to make this call to the Chief (...), who considered it appropriate. This call can be framed within the own management that is framed in Law 4/2015, of 30 March on the protection of public safety, in its article 16.
I then called the Chief of the Local Police of (...) explaining the reason for my reasonable doubts, within the access checks to a security compound such as the ISPC and with alert level 4 in the that we meet (...)".

5. On 04/05/2019, also during this preliminary information phase, a new request was made to the ISPC in order for the following to be answered:

- The complainant complained that the data that would have been the subject of consultation in relation to his person would be the following: a) data included in an appeal that the complainant here would have filed in the year (...) against a resolution dictated by the ISPC; and, data relating to courses that the complainant here had taken at the ISPC (course taken in (...) of 2018 on the use of firearms). Given the above, the ISPC was asked to answer the following questions:
  • Detailed information on the retention periods and filing system in relation to the following documentation: a) proceedings files (whether administrative or administrative contentious) to which the ISPC has been a party, especially with regard to those that they started at (...) (as it would be the one to which the complainant alludes); and, b) academic records of courses taken at the Police School of Catalonia.
  • Indicate the people who would have access to the cited information (administrative and/ or contentious proceedings files and academic files), whether they are kept - if so - in physical or electronic format. • If the ISPC has implemented some type of control or registration (either manual or automated) that allows knowing the specific people who have been able to access the information mentioned in the previous sections. If so, indicate the people who from 12/01/2018 to 02/15/2019 would have accessed this information and justify the reasons for each of the accesses.

- In relation to the call made by (...) to the head of the Local Police of (...), it is necessary to indicate whether the functions of this command include that of guaranteeing the safety of people and ISPC facilities. If so, indicate the rule that provides for it.

6. On 04/18/2019 the ISPC responded to this last request, through a report issued by (...)(...) of the ISPC, in which, among other relative points to the terms of conservation, filing systems and conditions of access to the records of administrative resources and

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

contentious and academic files, which do not affect the present procedure, was exposed which, in accordance with article 3 of Decree 160/2016, of 2 of (...), restructuring the Public Security Institute of Catalonia, corresponds to the Area (...) of the Police -to which belongs the sub-inspector who made the call to the head of the Local Police of (...), superior of the complainant here- guarantee the safety of people and the facilities of the Institute of Public Security of Catalonia.

7. On 06/03/2020, an archive resolution was issued regarding the reported conduct related to possible access to the files linked to the reporting person contained in ISPC files. In that resolution, the reasons that led to its archive were justified.

On that same date, the director of the Catalan Data Protection Authority agreed to initiate disciplinary proceedings against the ISPC for an alleged infringement provided for in article 83.5.a), in relation to article 5.1.f) ; both of Regulation (EU) 2016/679 of the European Parliament and of the Council, of April 27, relating to the protection of natural persons with regard to the processing of personal data and the free movement thereof (hereinafter, RGPD); for the conduct described in the proved facts section of this proposal. Likewise, she appointed Mrs. (...), an employee of the Catalan Data Protection Authority, as instructor of the file. This initiation agreement was notified to the imputed entity on 03/11/2020.

8. In the initiation agreement, the accused entity was granted a period of 10 working days, counting from the day after the notification, to formulate allegations and propose the practice of evidence that it considered appropriate to defend their interests.

9. On 10/06/2020, the ISPC made objections to the initiation agreement, which are addressed in section 2 of the legal basis.

proven facts

In the month of (...) of 2019 the sub-inspector sub-head of the Area (...) of the PG-ME, which provides services to the ISPC, contacted by telephone the head of the Local Police of the City Council of (...), superior of the person reporting here who belongs to this police force. In the course of this conversation, the sub-inspector revealed information relating to the complainant here, specifically, that he was going to study in the library (Security Knowledge Center) of the ISPC at a time that would seem incompatible with the shifts usual of an active police officer.

Fundamentals of law

1. The provisions of the LPAC, and article 15 of Decree 278/1993, according to the provisions of DT 2a of Law 32/2010, of October 1, of the Authority

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

Catalan Data Protection Authority. In accordance with articles 5 and 8 of Law 32/2010, the resolution of the sanctioning procedure corresponds to the director of the Catalan Data Protection Authority.

2. As stated in the antecedents (7th antecedent), this Authority agreed to initiate a sanctioning procedure against the ISPC, for a presumption provided for in article 83.5.a), in relation to article 5.1.f); both of the RGPD.

However, having carefully assessed the allegations made by the entity denounced in the initiation agreement, it is considered that there are not sufficient indications to support the imputation to the ISPC of a violation of the principles relating to the treatment established in article 5 of the RGPD.

The ISPC essentially bases its defense on the fact that the processing of the data of the person reporting here was necessary in order to *"prevent a possible real and serious danger to public security and for the repression of facts constituting a possible crime or misdemeanour",* danger caused - according to the ISPC - by the *"bad conduct"* that the complainant here observed when he went as a user to the CCS, located in a security compound like the ISPC. He also adds that the controversial call was made *"by a person who has been assigned the competence, by a rule with the rank of law, to guarantee the safety of people and ISPC facilities".*

Data processing carried out by security forces and bodies for the investigation and prevention of crimes is not governed by the RGPD, but by Directive (EU) 2016/680, of the European Parliament and of the Council, of April 27, relating to the protection of natural persons with regard to the processing of personal data by the competent authority for the purposes of prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal sanctions, and free circulation of this data. To the extent that this Directive (EU) 2016/680 has not been transposed into national internal law within the period provided for that purpose (05/06/2018), the provisions of transitional provision 4a of the Organic Law 3/2018, of December 5, on the protection of personal data and guarantee of digital rights (hereinafter LOPDGDD), which establishes that these treatments will continue to be governed by the Organic Law 15/1999, of December 13, on the protection of personal data (hereinafter, LOPD), and in particular by article 22, and its development provisions, until the rule transposing the Spanish law what the aforementioned directive provides.

Article 22 of the aforementioned LOPD, dedicated specifically to the files of the Forces and the Security Forces, foresees the following:

"The collection and processing for police purposes of personal data by the Forces and Security Bodies without the consent of the affected persons are limited to those cases and those categories of data that are necessary for the prevention of a real danger to public security or for the repression of criminal offences, i

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

they must be stored in specific files established for this purpose, which must be classified by category depending on the degree of reliability".

The processing of the data carried out by the PG-ME, without the consent of the affected person, will be lawful - under the terms provided for in Directive (EU) 2016/680 - to the extent that it fits the assumptions established in the article 22 of the LOPD, that is, when the treatment is limited *"to those cases and those categories of data that are necessary for the prevention of a real danger to public security or for the repression of criminal offences".*

The consideration that a personal data has been treated for police purposes is therefore crucial, given that this circumstance depends, as has been said, on the applicability of article 22 of the LOPD as a rule that would enable its treatment . In relation to what is to be understood by police purposes, Recommendation nº (87)15 of the Council of Europe, which regulates the use of personal data for police purposes, explains the following in its appendix : *the expression for police purposes includes all the tasks for which the police authorities must act for the prevention and suppression of crime and the maintenance of public order".* Also the wording of article 22.2 of the LOPD clearly defines the concept of data for police purposes: they will be those necessary for the prevention of a real danger to public security or for the repression of criminal offences.

Well, in the case at hand, and in view of the demonstrations made by the ISPC, both in the preliminary information phase and in the course of this procedure, it would be forced to consider that the behavior that here complainant observed in the ISPC effectively endangered public safety or could constitute a criminal offence. In fact, in the report issued by the sub-inspector (...) - to which the ISPC refers in its allegations -, he states that the conduct of the complainant here was *"inappropriate"* and that *"violated the general rules of respect for coexistence, other users and the correct use of the ISPC facilities, among which it is worth noting inappropriate behavior in verse (...);* referring only tangentially to the security alert. To the above, it should be added that the ISPC has not proven to have formally initiated any police procedure linked to the behavior observed by the complainant here, a procedure that logically should have been initiated if this behavior had really been so serious as to endanger people or facilities.

Discarded therefore that it is proven that the processing of the disputed data was necessary *"for the prevention of a real danger to public security or for the repression of criminal offenses" (ex art. 22 LOPD),* it would be application of the RGPD in the event that the data have been used for other purposes. It is therefore necessary to resolve whether the treatment - in this case the communication - of the data of the complainant here has a legitimate basis that grounds it.

In this case, the legal basis established in article 6.1.e.) of the RGPD is of interest, which enables the processing of data when *"The treatment is necessary for the fulfillment of a mission carried out in public interest or in the exercise of public powers conferred on the person responsible for the treatment".*

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

As can be seen from article 6.3 of the RGPD, the legal basis for the treatment indicated in letter e) must be established by European Union Law or by the law of the Member States that applies to the person in charge of the treatment .

Article 62 of the LPAC establishes the following in relation to *the "Initiation of the complaint procedure":*

"1. Complaint is understood as the act by which any person, whether in compliance with a legal obligation or not, brings to the attention of an administrative body the existence of a specific fact that can justify the initiation of ex officio an administrative procedure.
2. Complaints must express the identity of the person or persons presenting them and the account of the facts brought to the attention of the Administration. When the aforementioned facts may constitute an administrative infraction, they must collect the date of their commission and, when possible, the identification of those allegedly responsible (...)"

And article 13.1 of Decree 179/2015, of August 4, which approves the Regulation of the procedure of the disciplinary regime applicable to the local police forces of Catalonia, determines that the complaint, among others, is one of the means that can lead to the ex officio initiation of a disciplinary procedure *("The disciplinary procedure is always initiated ex officio, by agreement of the competent body, or by initiative own or as a result of a superior order, reasoned request from subordinates or complaint").*

Well, it is in accordance with these precepts that the communication of the disputed data by the ISPC to the Local Police of (...) should be understood as enabled. As stated in the proceedings, the ISPC was aware that the complainant was a member of the local police of (...), since in order to access the CCS of the ISPC, he had had to be accredited as a member of a police force (in accordance with the *"Informative Note"* of 20/03/2019 issued by the Deputy Director (...), transcribed in part in the 4th antecedent). On the other hand, it is necessary to take into account, as the ISPC also stated in its report of (...) of 03/21/2019 (also in part in the 4th antecedent), *"the fact that his assistance in the CCS was continues in the morning and afternoon from Monday to Friday, which could be contradictory to the usual shifts of an* active police officer. Well, it is this apparent "incongruity" between the status of an active member of the local police and the continued presence in the CSS - from which an eventual breach of duties could be inferred - which would justify - based on the rules cited - that the ISPC bring to the attention of the Local Police of (...) this fact and related information, so that this police force could evaluate the opportunity to initiate actions with the aim and effect of resolving eventual disciplinary responsibilities.

In short, given the specific circumstances of the case that is the subject of this resolution and the considerations set out, it is not possible to uphold the charge initially formulated against the ISPC.

Carrer Rosselló, 214, esc. A, 1r 1a
08008 Barcelona

Consequently, the present procedure should be postponed in accordance with article 20.1.a) of Decree 278/1993, of November 9, on the sanctioning procedure applied to the areas of competence of the Generalitat of Catalonia.

resolution

For all this, I resolve:

1. Declare the dismissal of sanctioning procedure no. 10/2020, referring to the Public Security Institute of Catalonia.

2. Notify this resolution to the Public Security Institute of Catalonia. and the reporting person.

3. Order that this resolution be published on the Authority's website (www.apd.cat), from in accordance with article 17 of Law 32/2010, of October 1.

Against this resolution, which puts an end to the administrative process in accordance with articles 26.2 of Law 32/2010, of October 1, of the Catalan Data Protection Authority, and 14.3 of Decree 48/2003 , of 20 of (...), by which the Statute of the Catalan Data Protection Agency is approved, the interested persons can file, with discretion, an appeal for reinstatement before the director of the Catalan Authority of Data Protection, within one month from the day after its notification, in accordance with the provisions of article 123 et seq. of the LPAC. They can also directly file an administrative contentious appeal before the administrative contentious courts, within two months from the day after their notification, in accordance with articles 8, 14 and 46 of Law 29/1998, of July 13, regulating the administrative contentious jurisdiction.

Likewise, interested parties can file any other appeal they consider convenient to defend their interests.

The director,