Carrer Rosselló, 214, esc. A, 1st 1st
08008 Barcelona

File identification

Archive resolution of the previous information no. IP 351/2018, referring to the City Council of (...).

Background

1. On 14/12/2018, the Catalan Data Protection Authority received a letter from a union section in which it filed a complaint against the City Council of (...), on the grounds of an alleged non-compliance with the regulations on the protection of personal data.
The reporting entity stated that the City Council carried out the following processing of personal data:

1.1 The recording of calls from the Urban Guard.
1.2 The recording of conversations held through the transmission equipment assigned to each agent.

1.3 The geolocation of the agents' communication terminals.
1.4 The focus of a workplace through the camera located in the public attention area of the police stations.

In relation to all these treatments, the reporting entity questioned whether it was necessary to have an access register, in which the motivation for the consultation was stated. In turn, with regard to the recording of telephone calls and the images captured by the video surveillance system installed in the police stations, the reporting entity was also wondering what was the term for keeping the data. Likewise, the reporting entity inquired whether the person who has access to the recorded calls "he has opened one file the call a some worker is he has the obligation to save it and attach it to the file" where a proof, and whether the images captured by the video surveillance system can be used for disciplinary purposes. In turn, the reporting entity indicated that the camera located in the public attention room (operator's room) of the police station, would focus on the workplace of the agent assigned there. And in the last one, the reporting entity stated that the City Council had a security document, which it would like to access.

The reporting entity provided various documentation.

2. The Authority opened a preliminary information phase (no. IP 351/2018), 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.

Carrer Rosselló, 214, esc. A, 1st 1st
08008 Barcelona

3. On 21/02/2019 and 01/03/2019, the reporting entity supplemented its letter of complaint. In summary, he stated the following there:

3.1 That Corps Order 5/2017 stated that one of the cameras was at the entrance to the police stations, but its location was in the operator's room, as stated in the corresponding report.

3.2 That it was unknown whether the file had been registered.

3.3 That the memory of the video surveillance system indicated that "Is not they place cameras that focus on jobs."

3.4 That the Chief Inspector of the Urban Guard stated before the "Court nº 1, Previous 202/2018" which had images referring to the representative of the complaining trade union section.

3.5 That the Chief Inspector could view the images captured by the video surveillance system installed in the police stations through his mobile phone.

3.6 That the administrator of the company installing the cameras would be the brother of the Chief Inspector, so he considered that there was an alleged crime of embezzlement and embezzlement of public funds.

The reporting entity provided various documentation.

4. In this information phase, on 04/16/2019, the Authority carried out an inspection at the premises of the Urban Guard in (...), to verify certain aspects related to the treatments carried out by the Urban Guard. In that act of inspection
in person, the representatives of the City Council of (...) stated, among others, the following:

4.1 About the calls and the broadcaster:

- That it was not known whether the program that captured calls, incoming and outgoing, through the number of the Local Police, was working.
- That the calls that could be recorded would be those made or maintained through the number (...) (Urban Guard telephone) and the women's helpline ((...)).
- That with respect to the communications made through the police station, it was not known whether the recording of the calls was active.
ÿ That the system for recording calls through the aforementioned numbers and communications made through the Local Police station was the same.
- That the person authorized to access said system was the Chief Inspector of the Urban Guard.

4.2 About the geolocation of the radio stations of the Urban Guard:

- That the police communications terminals (station) allowed geolocation.
- That these terminals are from the RESCAT network and allow geolocation through SIPCAT.

Carrer Rosselló, 214, esc. A, 1st 1st
08008 Barcelona

- That these devices have been available for 6 years.
- That geolocation was out of use, given that it often failed.
- That geolocation was in the testing phase for a few days in the summer of 2018. After a while it went offline.
- That the purpose of geolocation was to guarantee the safety and integrity of the staff and the adequate provision of police services.
- That it had not been used for disciplinary purposes or labor control.
- That the users who were authorized to access the geolocation were the Chief Inspector since its inception and a certain sergeant since the summer of 2018. The ward agent had access to the geolocation, given that it could only be consulted through the monitor located in the control room.
- That it was unknown if there was a log of accesses.

4.3 About the camera installed in the public service room (operator):

- That the camera was installed in 2017.
- That it was not known whether the camera allowed to expand the field of focus (zoom).
- That the retention period of the images was unknown.
- That the purpose of processing images through said camera is to guarantee the safety of the facilities and the agents. The installation took place following the terrorist alert.
- That it was unknown whether the images captured for disciplinary or labor control purposes had been used or were planned to be used.
- That it was not known whether any recording of images captured through the video surveillance system, referring to the representative of the reporting entity, was preserved.
- That the user who was authorized to access the real-time or recorded images was the Chief Inspector.
- That it was unknown if the images could be viewed remotely.

Likewise, the Authority's inspection staff verified, among others, the following:

- That there was a video surveillance camera in the operator's or control room. At the same time, it was also found that on the protective glass of the control room there was an informative poster about the existence of the camera, which was visible from the outside of said room.
- That the monitor, where the representatives of the inspected entity stated that geolocation was viewed, was disconnected.
ÿ That in the communications cabinet (RAC) of the police departments, where the server was, there were several numbered exits, among them number 21. According to the representatives of the City Council, these exits allowed the connection between the server and the various physical connection points of the computer equipment (network connections) distributed by the police departments that make up their internal network. In turn, the inspector staff found that one of the physical connection points located on the 2nd floor of the police offices was numbered.

Carrer Rosselló, 214, esc. A, 1st 1st
08008 Barcelona

Finally, the inspection staff required the inspected entity to report on several aspects linked to the events reported.

5. On 05/22/2019, the City Council of (...) complied with this request by means of a letter stating the following:

5.1 About calls and the station:

- That on 28/01/2013, a telephone and radio voice recording system was installed in the RAC of the Urban Police.
- That, on 23/04/2019, it had been verified that only incoming and outgoing calls made to the telephone number (...) (Urban Guard telephone number) were recorded. In other words, the recording was limited only and exclusively to calls made or received from the operator's room.

ÿ That the purpose of this treatment is to verify and conveniently record the demands of users of the police service; as well as the response and treatment that the agent - operator provides to the request in question, in cases where there is a risk to public safety.
- That the recorded conversations had not been used for disciplinary or labor control purposes.

- That the maximum storage period is 30 days.
ÿ That in relation to the analysis of risks to determine the appropriate security measures to mitigate them, the City Council was working on the progressive adaptation of the new legislation on data protection, which included an analysis of the risks.
ÿ That the call log could be accessed, but there was no record of who had accessed it since there was only one official authorized to access it. Since 23/04/2019, three officials (Commands of the Urban Guard) had been registered as authorized users. In turn, he added that there was a record of the user's identification and the day and time, but not of the call being consulted.

- That it was not verified afterwards if these were necessary for the exercise of their functions and for the declared purpose.
- That in relation to the numbers (...) and (...), there was no connection with the recorder.

5.2 About the geolocation of the radio stations of the Urban Guard:

- That the system through which the geolocation could be consulted, was not audited and had no record of user entries and exits.
- That prior to the testing period (summer 2018), geolocation was not active. Tests had only been carried out to verify its correct operation, with negative results. Further tests were carried out from summer 2018, but as the errors persisted, the system was permanently taken offline.

Carrer Rosselló, 214, esc. A, 1st 1st
08008 Barcelona

5.3 About the camera installed in the public service room (operator):

- Given the internal capacity of the hard disk, the maximum recording time is approximately 20 days, after which the images are deleted automatically.
- That, on 04/18/2019, it was verified that there was no recording corresponding to the month of March 2019, and the records started on 04/01/2019 (photographs were provided to prove this verification).

- That the recordings are kept in the recorder located in the RAC of the computer system. They could be viewed by the Chief Inspector of the Urban Guard.
- That they had not been used, nor was it planned to use the images captured by said camera for disciplinary or labor control purposes. The exclusive purpose is to guarantee the security and internal or external protection of these dependencies, especially at a time of terrorist alert level 4 out of 5.

- That no recording of images captured through the video surveillance system, referring to the representative of the reporting entity, is preserved.
- That the images can be viewed from the computer installed in the Chief of Staff's office, and remotely from the Chief Inspector's mobile phone.
- That to view the images through the mobile phone, a password must be entered to be able to access the application (a screenshot was provided). Images are encrypted and watermarked to ensure that no unauthorized person can access them.
- That it was not recorded that there was an access register, since there was only one person authorized to access the images.
- That it was not verified afterwards if these were necessary for the exercise of their functions and for the declared purpose.

The City Council of (...) provided a copy of the images recorded on 04/15/2019, between 9:00 a.m. and 9:02 a.m.

6. Based on the antecedents that have been related and the result of the investigative actions carried out within the framework of the previous information, today an agreement has been issued to initiate disciplinary proceedings regarding the reported conduct related to the field of vision of the camera installed in the room of the operator of the Urban Guard; and with the security of the data, for not having carried out a risk analysis to determine the appropriate security measures to be applied in the treatments linked to geolocation; to the video surveillance system and the recording of telephone conversations and transmission equipment.

The rest of the reported conduct and other inquiries from the complainant are addressed in this file resolution.

Fundamentals of law

Carrer Rosselló, 214, esc. A, 1st 1st
08008 Barcelona

1. In accordance with the provisions of articles 90.1 of the LPAC and 2 of Decree 278/1993, in relation to article 5 of Law 32/2010, of October 1, of the Authority Catalan Data Protection Agency, and article 15 of Decree 48/2003, of February 20, which approves the Statute of the Catalan Data Protection Agency, the director of the Catalan Data Protection Authority.

2. Based on the account of facts that has been set out in the background section, it is necessary to analyze the reported facts that are the subject of this file resolution.

2.1. About security measures.

In this regard, the reporting entity questioned whether, in order to access the telephone conversations held through the station, the geolocation and the images recorded by the video surveillance system installed in the police stations, there was a record of 'accesses where what was accessed, the date and the reason were saved.

In the framework of the previous actions, the reported entity has indicated the information that is registered with respect to each access, in the cases where an access register had been implemented (in the recording of telephone conversations and of the broadcaster ).

Having said that, it should be borne in mind that it is up to the person in charge of the treatment to assess the risks inherent in the treatment and thus determine the appropriate measures to guarantee the security of the data, among which, there could be the access register (in which keep the information that is considered appropriate to guarantee security).

Therefore, without having carried out this assessment, it is not possible to determine whether this measure (and its scope) indicated by the reporting entity is appropriate to guarantee the security of the data. In this regard, it should be borne in mind that it has been agreed to start the corresponding sanctioning procedure, and one of the infractions charged there is that of not having carried out said risk analysis.

2.2. About the data retention period and blocking.

In the letter of complaint dated 12/14/2018, regarding the recording of telephone calls and the images recorded by the video surveillance system, the reporting entity raised the question of what would be the period of data conservation and whether this was correct

Article 5.1.e of the RGPD regulates the principle of limiting the retention period, determining that personal data "maintained in a way that allows identification for longer than necessary interested during non- for the purposes of data processing personal; personal data longer periods as long as they are exclusively for archival purposes public interest, scientific research purposes or historical statistical purposes, in accordance with article 89, section 1, without prejudice to the

Carrer Rosselló, 214, esc. A, 1st 1st
08008 Barcelona

application of the appropriate organizational and technical measures to guarantee a level of security adequate to the risk, in order to protect the fundamental rights of the interested party" and in order Regulation ay

Therefore, the data controller must keep the data for the period strictly necessary to achieve the intended purpose.

In the present case, the City Council of (...) has informed that the maximum storage period for incoming and outgoing calls made through the number (...) is 30 days at most; as well as the effective retention period of the images captured by the video surveillance system is 18 days (although the forecast was that the images would be retained for 20 days).

Given the above, it is considered that said retention periods are adequate to achieve the intended purposes. In fact, in application of the principle of limiting the term of data conservation, article 22.3 of Organic Law 3/2018, of December 5, on the protection of personal data and guarantee of digital rights (LOPDGDD), establishes that :

"The data must be deleted capture, the maximum period of one month from the en his except when the commission of acts must be put to of seventy-two hours after becoming aware of the existence of the recording facilities or (...)"

in one case, maximum term is of

Having established the above, it is necessary to address whether there is any obligation to preserve telephone calls when these may constitute evidence, as proposed by the reporting entity in its letter of complaint.

In this regard, article 32 LOPDGDD should be invoked. The first three sections of this precept provide the following:

"1. The person responsible for the treatment is a lock data when in term year obliged to rectify the deletion.
have identification 2.
The blocking of the data consists of the measures, the treatment and only for the limitation period of these. a

in of a

After this period, the data must be destroyed.
3. The blocked data indicated in is not they can treat for no purpose other than the the previous section."

That being the case, the data controller is obliged to block the data when they have to be rectified or deleted, with the sole purpose of making them available to judges and courts, the Public Prosecutor's Office or the competent public administrations (among them , the data protection authorities), for the requirement of possible responsibilities that may arise during the limitation period of these.

Having said that, it should be specified that in the case of treatments for video surveillance purposes, the LOPDGDD has established that the blocking obligation is not applicable (article 22.3).

2.3. About the eventual initiation of a disciplinary file and the security document.

Then, in its letter of 14/12/2018, the reporting entity raises a hypothetical case, in which the images captured by the video surveillance system installed in the police stations were used for disciplinary purposes. And, on the other hand, it was stated that the City Council had a security document in relation to the video surveillance system, to which the reporting entity stated that it wanted to access.

With regard to these questions, it is necessary to demonstrate that no specific fact is being reported that involves the possible commission of a specific infringement of the regulations on data protection, but that they are in the scope of consultation or mere hypothesis, reason which is why it is not necessary to analyze them. It is for this reason that it becomes unnecessary to address them.

2.4. About the location of the cameras.

In its letter of 01/03/2019, the reporting entity stated that in Corps Order 5/2017 it was indicated that one of the cameras was at the entrance to the police stations, but its location was in the operator's room, as stated in the corresponding report.

Well, Body Order 5/2017 of 05/16/2017 reported that a video surveillance system had been acquired and that the controversial camera would be installed in the "Entrance Prefecture, focusing on the public attention area" .

Subsequently, in the report on the video surveillance system of the police stations, drawn up on 22/05/2017 by the City Council in compliance with the provisions of article 10 of Instruction 1/2009, it was specified that that camera would be installed "in the office of the operator of the Local police".

That's how things are, after Body Order 5/2017, the City Council of (...) considered installing the camera in another location (in the operator's room).

This change in the location of the controversial camera does not indicate any conduct contrary to the regulations on data protection.

Carrer Rosselló, 214, esc. A, 1st 1st
08008 Barcelona

Having said that, it should be noted that the regulations on data protection do not require that the affected people be informed about the specific location of the cameras.

On the other hand, the reporting entity stated that, in the aforementioned report, the Chief Inspector "manipulates the report, since he frames what he wants and what the camera is not really focusing on" .

In relation to the above, certainly in article 10.1.e) of Instruction 1/2009 it is pointed out that the report must refer to the location and field of view of the cameras.

Well, in the same report prepared by the City Council on 05/22/2017, in relation to the field of focus of the cameras, the following was specified: "Indicative viewing: photos made with iPhone" .

It is worth saying that the fact that the report includes this indicative viewing is not contrary to the regulations on data protection. And this, because this report must be drawn up prior to the start-up of the video surveillance system (art. 10.1 of Instruction 1/2009).

Having established the above, it must be taken into account that it has been agreed to start the corresponding sanctioning procedure in relation to the scope of vision of this camera.

2.5. About authorization and file.

At this point, also in the letter of 03/01/2019, the reporting entity stated that it did not know whether the video surveillance system had been authorized by the Video Surveillance Devices Control Commission of Catalonia (hereafter CCDVC), as well as whether the corresponding file had been notified to the Authority.

First of all, article 7.2 of Decree 134/1999, of 18 May, regulating video surveillance by the police of the Generalitat and the local police of Catalonia (hereinafter, Decree 134/1999) establishes that the installation of a fixed video surveillance system by the local police, apart from being authorized by the General Directorate of Security Administration of the Department of the Interior, requires a prior favorable report from the CCDVC.

However, article 1.3 of Decree 134/1999 provides that when the purpose of the cameras is to guarantee security and internal or external protection in buildings, outbuildings or facilities of the local police, as happens in the in the present case, in relation to the treatments carried out in said police precincts, the aforementioned sectoral regulations do not apply.

Therefore, in the present case the favorable report of the CCDVC is not required.

Carrer Rosselló, 214, esc. A, 1st 1st
08008 Barcelona

And secondly, with regard to the notification and registration of the file with the Authority, it must be pointed out that the RGPD has removed this obligation.

2.6. About access to images.

In this regard, the reporting entity explained that, in judicial proceedings, the Chief Inspector would have declared that he had images of the person representing the reporting entity captured by the camera located in the operator's room. Given the above, he requested the Authority to ask the City Council for a copy of said images.

First of all, it must be made clear that this request must be formalized by means of an access request that, the interested person, must address to the person responsible for the treatment (the City Council) in accordance with the provisions of the article 15 RGPD. And in the event that the City Council does not respond to this request or the response is not satisfactory, the interested person can submit a claim to the Authority.

Without prejudice to the above, by means of a letter dated 21/05/2019, the City Council of (...) stated that the images referred to were not preserved.

2.7. About viewing images via mobile.

At this point, the reporting entity stated that the Chief Inspector could view the images captured by the video surveillance system.

In this regard, by means of a letter dated 21/05/2019, the City Council of (...) informed that the Chief Inspector was the only person authorized by the Council to access the images captured and recorded by the system of video surveillance installed in police stations; as well as that he could view them through his computer located in the police stations and, remotely, through his mobile phone.

In turn, he pointed out that to view the images through the mobile phone it is necessary "enter one and access password to the application, the images are encrypted and watermarked, authorized for one a no the same."

That being the case, access by an authorized person to the images captured and recorded by the video surveillance system, or remotely, in the exercise of their duties, is not contrary to data protection on site

Another thing is whether this treatment guarantees the security of the data. In this sense, it is necessary to carry out the risk analysis, the lack of which is imputed to the City Council in the sanctioning procedure that has been initiated.

Carrer Rosselló, 214, esc. A, 1st 1st
08008 Barcelona

2.8. About criminal acts.

Finally, in its letter of 01/03/2019, the reporting entity stated that the administrator of the company installing the cameras would be the brother of the Chief Inspector, so it considered that could have committed an alleged crime of embezzlement and embezzlement of public funds.

In relation to the above, it is sufficient to indicate that this Authority is not competent to decide whether or not these facts constitute a crime.

3. In accordance with everything that has been set out in the 2nd legal basis, and given that during the actions carried out in the framework of the previous information it has not been accredited, in relation to the facts that have been addressed in this resolution, no fact that could be constitutive of any of the infractions provided for in the applicable legislation, should be archived.

resolution

Therefore, I resolve:

1. File the actions of prior information number IP 351/2019, relating to the City Council of (...), in relation to the facts referred to in the legal basis 2n.

2. Notify this resolution to the City Council of (...) and communicate it to the reporting entity.

3. Order the publication of the resolution on the Authority's website (www.apd.cat), 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 article 14.3 of Decree 48/2003, of 20 February, which approves the Statute of the Catalan Data Protection Agency, the denounced entity can file, with discretion, an appeal for reinstatement before the director of the Catalan Data Protection Authority, within one month from the day after its notification, in accordance with the which provides for article 123 et seq. of Law 39/2015. You can also directly file an administrative contentious appeal before the administrative contentious courts, within two months from the day after its notification, in accordance with articles 8, 14 and 46 of Law 29/1998, of July 13, regulating the administrative contentious jurisdiction.

Likewise, the reported entity can file any other appeal it deems appropriate to defend its interests.

The director,