IAI 74/2021

Report issued at the request of the Commission for the Guarantee of the Right of Access to Information Public in relation to the claim submitted for the denial of access to the internal file, the conclusions and the sanctions imposed in relation to the case of impersonation in a police force

The Commission for the Guarantee of the Right of Access to Public Information (GAIP) asks the Catalan Data Protection Authority (APDCAT) to issue a report on the claim presented by a parliamentary group against the Administration for the denial of access to the internal file, the conclusions and the sanctions imposed in relation to the case of impersonation in a police force.

Having analyzed the request, which is accompanied by a copy of the administrative file processed before the GAIP, and in accordance with the report of the Legal Counsel, I issue the following report:

Background

1. On May 21, 2021, a member of a parliamentary group urges a parliamentary question addressed to the councilor in which, given the case uncovered by a media outlet regarding impersonation originating in a police force, report on which internal investigations have been carried out, what are the results of these and what measures have been taken. It also requests "the internal file if it was opened, its conclusions and the sanctions imposed if there were any, as well as any other action that has been taken in this regard."

2. On July 6, 2021, the Department responds that it initiated a classified information, which resulted in the initiation of a disciplinary file, ending with the imposition of a penalty. And, regarding the request for access and copy of the file in question, the request is denied in application of article 23 of Law 19/2014, of December 29, on transparency, access to public information and good governance (LTC).

3. On July 26, 2021, another member of the same parliamentary group files a complaint with the GAIP against the Department for denying access to information requested public

4. On July 29, 2021, the GAIP forwards the claim to the Department, informing it of the processing of the mediation procedure at the express request of the complaining party, and requiring the issuance of a report in which they base their positions, as well as the complete file relating to the request for access to public information, the identification of third parties who are affected by the requested access, as well as the person or persons who will represent the Department at the mediation session.

5. On August 24, 2021, the first mediation session will be held in which, given the mediator's proposal to deliver the requested information in an anonymized manner, the session will be suspended so that the parties can assess this proposal .

6. On September 3, 2021, the second mediation session will be held in which, although the complaining party agrees to be provided with the file prior to anonymization of the personal data, the Department argues that it is not possible to be affected by the limit relating to public security, so the mediation procedure must be resolved by resolution of the GAIP Plenary.

7. On September 3, 2021, the GAIP will write to the person making the claim in order to confirm their agreement to receive the anonymized information, excluding the personal data of the people that may appear in it, including the TIP number of the agents that can be identified.

8. On September 8, 2021, the claimant sent an email to the GAIP stating the following:

> "We agree to receive the documentation excluding only the personal data that may be included.
> Under no circumstances can we agree to withdraw the TIPS numbers of the agents that may be listed there.
> The non-inclusion of TIPS collides head-on with the task of parliamentary control that we are obliged to exercise, as it prevents us from being able to verify and assess that the appropriate procedures have been followed in this file.
> Finally, we reiterate the need for the documentation to be delivered, in compliance with the data protection law, to contain exclusively personal data and not any other data from the file."

9. On September 8, 2021, the GAIP, in order to have the necessary elements to resolve the procedure, requires the Department to transfer a copy of the disciplinary file to a member of the police force or the possibility of in-person access to its offices to consult it.

10. On September 21, 2021, the Department will notify the GAIP of the contact person with whom to set a date and time for the consultation of the controversial file.

11. On October 20, 2021, the Department sends the report issued in relation to the claim submitted to the GAIP. In this report, and among other considerations, the application of the following limits on access to the requested file is made:

a) Limit relating to public safety (article 21.1.a) LTC).
b) Limit relative to the investigation or sanction of criminal, administrative or disciplinary (article 21.1.b) LTC).
c) Limit relating to privacy and other legitimate private rights (article 21.1.f) LTC).
d) Limit relating to the protection of data deserving of special protection (article 23 LTC).

12. On October 22, 2021, the GAIP requests this Authority to issue the report provided for in article 42.8 of Law 19/2014, of December 29, on transparency, access to public information and good governance, in relation to the claim presented.

Legal Foundations

I

In accordance with article 1 of Law 32/2010, of October 1, of the Catalan Data Protection Authority, the APDCAT is the independent body whose purpose is to guarantee, in the field of the competences of the Generalitat, the rights to the protection of personal data and access to the information linked to it.

Article 42.8 of the LTC, which regulates the complaint against resolutions regarding access to public information, establishes that if the refusal is based on the protection of personal data, the Commission must request a report to the Catalan Data Protection Authority, which must be issued within fifteen days.

For this reason, this report is issued exclusively with regard to the assessment of the incidence that the requested access may have with respect to the personal information of the persons affected, understood as any information about an identified or identifiable natural person, directly or indirectly, in particular through an identifier, such as a name, an identification number, location data, an online identifier or one or more elements of physical, physiological, genetic, psychological, economic, cultural or social security of this person (article 4.1 of Regulation 2016/679, of April 27, 2016, relating to the protection of natural persons with regard to the processing of personal data and the free circulation of such data and by which repeals Directive 95/46/EC (General Data Protection Regulation, hereafter RGPD).

Therefore, any other limit or aspect that does not affect the personal data contained in the requested information is outside the scope of this report, as is the case of the limits
established in article 21 of the LTC relating to public security (section 1.a)), to the investigation or sanction of criminal, administrative or disciplinary offenses (section 1.b)) and to privacy and other rights legitimate private parties (section 1.c)), to which the Department expressly refers, the application of which could lead to the claimant's right of access being denied or restricted.

The deadline for issuing this report may lead to an extension of the deadline to resolve the claim, if so agreed by the GAIP and all parties are notified before the deadline to resolve ends.

Consequently, this report is issued based on the aforementioned provisions of Law 32/2010, of October 1, of the Catalan Data Protection Authority and the LTC.

In accordance with article 17.2 of Law 32/2010, this report will be published on the Authority's website once the interested parties have been notified, with the prior anonymization of personal data.

II

Article 4.2) of the RGPD considers “treatment”: any operation or set of operations carried out on personal data or sets of personal data, either by automated procedures or not, such as collection, registration, organization, structuring, conservation , adaptation or modification, extraction, consultation, use, communication by transmission, diffusion or any other form of enabling access, comparison or interconnection, limitation, deletion or destruction.”

The RGPD provides that all processing of personal data must be lawful (Article 5.1.a)) and, in this sense, establishes a system of legitimizing data processing based on the need for one of the legal bases to be met established in its article 6.1.
Specifically, section c) provides that the treatment will be lawful if "it is necessary for the fulfillment of a legal obligation applicable to the person responsible for the treatment".

As can be seen from article 6.3 of the RGPD and expressly included in article 8 of Organic Law 3/2018, of December 5, on the protection of personal data and guarantee of digital rights (LOPDGDD), the processing of data it can only be considered based on this legal basis of article 6.1.c) of the RGPD when this is established by a rule with the rank of law.

For its part, article 86 of the RGPD provides that "the personal data of official documents in the possession of any public authority or public body or a private entity for the performance of a mission in the public interest may be communicated by said authority , organism or entity in accordance with the Law of the Union or Member States that applies to them in order to reconcile public access to official documents with the right to the protection of personal data under this Regulation.”

The regulation and guarantee of public access to official documents held by public authorities or public bodies is regulated in our legal system in the LTC.

The fifth additional Provision of this Law establishes the following:

"Five Specific regime of the Parliament of Catalonia

1. The Parliament of Catalonia, in accordance with the principle of parliamentary autonomy recognized by article 58.1 of the Statute of Autonomy, must make the amendments to the Regulations of the Parliament and its rules of regime and government interiors that are necessary to fulfill the requirements established by this law.

2. For the purpose referred to in paragraph 1, the Parliament must:

a) Update and expand the procedures for citizen participation in the law-making process, especially with the use of electronic media, in accordance with what is established in article 29.4 of the Statute.
b) Establish and regulate its own transparency portal.
c) Facilitate access to parliamentary documentation and information.
d) Provide information relating to the fulfillment of the obligations of deputies and senior officials in matters of incompatibilities, declarations of activities and assets and other obligations and duties related to their status, and also on their remuneration.
e) Facilitate public access to the curriculum vitae of persons proposed to occupy public positions whose appointment is the competence of the Parliament.

f) Define and develop the rules of good governance and open governance in the parliamentary sphere.
g) Create a register of self-interest groups.
h) Establish an own system of guarantees to ensure compliance with the obligations derived from this section, which must include at least the creation of a complaint body inspired by the principles established by Chapter IV of Title III .

3. Parliament must make the relevant regulatory adaptations to comply with what is established in section 2 before the entry into force of this law. The regulation established by the Parliament must determine the necessary adaptations derived from the institutional nature of the Parliament, which in no case can lead to a lower guarantee regime than that established by this law.

4.(...).”

Therefore, the specific legal regime to be applied to the right of access to information of members of the Parliament of Catalonia is that provided for in the Regulations of the Parliament of Catalonia (RPC).

III

Article 5 bis of the RPC provides the following:

"1. Deputies, in the exercise of their function, have the right to access information, and to obtain a copy, of the Administration of the Generalitat, of the bodies, companies and entities that depend on them and of the institutions and bodies of the Generalitat that act with functional independence or with a special autonomy recognized by law. Deputies can request this information directly or, if they consider it relevant, they can request it by communicating it to the president or through him.

2. The requested authorities or administration must provide the deputies with the requested information electronically or in writing.

3. The requested information must be delivered within fifteen days, extendable for a maximum of seven more days, starting from the day after the request has been communicated."

The administrative scope on which the right of access of the deputies of the Parliament of Catalonia is projected is determined by this article and covers the information of "the Administration of the Generalitat, the bodies, companies and entities that depend on it and of the institutions and bodies of the Generalitat that act with functional independence or with a special autonomy recognized by law".

In the case at hand, a member of a parliamentary group requests a copy of the disciplinary file issued to a member of the police force by the competent Department. This information remains subject to the regime of access recognized to deputies by article 5 bis of the RPC, transcribed.

However, article 5 ter of the RPC establishes that this right of access can be limited in certain cases:

"1. The right of access to information is part of the essential content of the representative and parliamentary function that corresponds to deputies and can only be limited by the concurrence of one of the restrictions established by the legislation regulating the right of access to information public

2. The right of access to the information of the deputies has, in any case, a preferential nature and must be able to be made effective whenever the rights or legal assets protected can be safeguarded through partial access to the information, the anonymization of sensitive data or the adoption of other measures that allow it."

This article expressly recognizes the applicability of the limits provided for in the regulations governing the right of access to public information, which are basically the limits established in the LTC.

In this regard, it should be borne in mind that article 22.1 of the LTC establishes that "the limits applied to the right of access to public information must be proportional to the object and purpose of the protection. The application of these limits must take into account the circumstances of each specific case, especially the concurrence of a higher public or private interest that justifies access to the information."

At this point, it should be noted that the right of access to information of members of Parliament is part of the essential content of the "ius in officium" or representative and parliamentary function recognized by Article 23.1 EC according to which "los ciudadanos tienen the right to participate in public affairs, directly or through representatives, freely elected in periodic elections by universal suffrage."

As stated, among others, STC 32/2017, "we are faced with "an individual right" of the Deputies that is integrated into the proper status of the position; right that: a) empowers them to collect information from the Regional Administration or "from the Central Administration, Local and other institutions in the territorial scope of Castilla-La Mancha" (art. 13.3); b) they are granted "for the best fulfillment of their functions"; c) its specific purpose is "to know certain facts and situations, as well as the administrative documents that evidence them, relating to the activity of public administrations; information that may well exhaust its effects in obtaining it or be instrumental and serve later so that the Deputy who receives it, or his parliamentary group, carry out a judgment or assessment on that specific activity and the Government's policy, using other instruments of control»

(STC 203/2001 (RTC 2001, 203) , FJ 3); yd) whose exercise only requires directing the request to the President of the Courts who will transfer it to the Bureau for its qualification in the manner provided for in article 32.1.4 (art. 13.2 of the Regulation) and that the information and documentation is necessary for the development of their tasks (art. 13.1 of the Regulation)."

It has also been recalled, in other judgments (SSTC 44/2010, 27/2011 or 28/2011), the relevance of the possibility of asking parliamentary questions, which is still a way of being able to request information. Thus, in STC 27/2011 it is stated: "In STC 44/2010, of July 26, the doctrine of this Court has been recalled in relation to parliamentary questions: "the faculty to formulate questions to the Government Council belongs to the core of the parliamentary representative function, since the participation in the exercise of the function of controlling the action of the Council of Government and its President and the performance of the rights and powers that accompany it constitute constitutionally relevant manifestations of the ius in officium of representative (SSTC 225/1992, of December 14 [RTC 1992, 225], F. 2;

107/2001 [RTC 2001, 107], F. 4; and 74/2009 [RTC 2009, 74], F. 3). Thus, the inadmissibility of the questions in question, if provided exceptionally in art. 153.2 RCV (LCV 2007, 6), supposes a limitation of the rights and powers that make up the constitutionally relevant status of political representatives whose first constitutional requirement is that such limitation appears sufficiently motivated (SSTC 38/1999 [RTC 1999, 38], F. 2; and 74/2009 [RTC 2009, 74], F. 3)" (F. 4).".

The consideration of this right of access of the deputies of the Parliament of Catalonia as preferred by article 5.2 ter of the RPC, the public interest linked to the exercise of the parliamentary function and the fact that this is an expression of the fundamental right to participate in Article 23 CE, means that deputies have a stronger position than that of citizens in general. Consequently, the limitations of the right of access will have to be interpreted even more restrictively.

Therefore, although the limits on access to information are the same in the regime of access to information for members of Parliament regulated in the RPC as in the general regime of access to information in legislation of transparency, it is necessary to weigh them according to what the jurisprudence has called the "essential plus" that must have access to the information of the deputies about the information available to any citizen, so that they can exercise the its representative function (STS of June 15, 2015).

So, when the information to which deputies request access contains personal data, as it happens in the case at hand, the eventual collision between the right of deputies to access said information and the right to the protection of personal data of those potentially affected, must be resolved in accordance with the criteria provided for in articles 23 and 24 of the LTC and with the principles of data protection regulations, taking into consideration the strengthened position of parliamentarians or the "essential added plus".

IV

In this case, a disciplinary file is requested against a member of a police force, which ended with the imposition of a penalty. The information contained in said file, referring to the sanctioned agent, is information deserving of special protection.

According to article 23 of the LTC, "requests for access to public information must be denied if the information sought contains particularly protected personal data, such as those relating to ideology , trade union membership, religion, beliefs, racial origin, health and sex life, and also those relating to the commission of criminal or administrative offenses that do not entail a public reprimand to the offender, except that the person affected expressly consents to it by means of a written document that must accompany the request."

In the same vein, article 15 of State Law 19/2013, of December 9, on transparency, access to public information and good governance (LT), provides:

> "1. If the requested information contains personal data that reveal the ideology, trade union affiliation, religion or beliefs, access can only be authorized if there is the express and written consent of the affected person, unless said affected person had made it manifestly public the data before access was requested.

If the information includes personal data that refers to racial origin, health or sex life, includes genetic or biometric data or contains data related to the commission of criminal or administrative offenses that did not lead to a public reprimand to the offender, access only it may be authorized if the express consent of the affected person is counted or if the latter is covered by a rule with the force of law."

This Authority has had the opportunity to analyze the application of the limit provided for in article 23 of the LTC and article 15 of the LT when the information to which the deputies want to access contains data deserving of special protection in CNS opinion 16/2019. This opinion concludes that:

"A strict application of article 23 of the LTC to any request for information of this nature interested by a deputy in the exercise of his position, would mean having to restrict access to the same without making any further assessment for the mere fact of being considered for transparency purposes to be particularly protected, and would in any case require the prior consent of the person concerned.

(...)

As this Authority already held in opinion CNS 5/2009, prior to the approval of the LT and the LTC, the application of the limit provided for in article 23 LTC in relation to access to information on the part of the deputies must necessarily lead to excluding the possibility of general access to the information on citizens to which this article grants special protection.

This must be the general criterion from which to start. However, it should also be borne in mind that the interpretation that is made of the applicability of the limits provided for in the LTC must be done in the light of the peculiar position held by the deputies due to the functions entrusted to them , in particular, for its function of controlling the Government.

A restrictive interpretation of the limitation provided for in article 23, placed in relation to the functions attributed to Parliament, and the preferential nature of the right of access in this area, does not allow us to rule out that there may be cases in which the information that is requested is related to actions of officials or public employees in the exercise of their functions, and that is essential for the deputies to be able to exercise their function of controlling government action. We think, for example, that even in the case of information that has been declared or reserved, article 11 of the RPC allows access, under certain conditions, to representatives of parliamentary groups. Absolutely limiting the access of deputies to the information referred to in articles 15.1 LT and 23 LTC could prevent the exercise of the specific function of controlling the Government's actions that the EAC attributes to Parliament, emptying of content the citizen's right to participate in public affairs through their representatives, which could be unjustified.

It will therefore be necessary to bear in mind that from the perspective of data protection regulations, the limitation of article 23 LTC (and 15.1 LT) would not allow generalized access to the

citizen information referred to in this article, although the access of deputies to certain information referred to in these articles cannot be ruled out, always with restrictive criteria, in particular when it refers to public positions that they are subject to the control of the Parliament, which may be essential for the exercise of the functions attributed to the Parliament."

In view of these considerations, in the face of a request for access by deputies such as the one being examined, which refers to a disciplinary procedure instructed by the Department to an agent, given that the information would contain categories of specially protected data, it would be necessary to limit access to this information, unless, given the preferential nature of the right of access of deputies, in the specific case said information can be considered essential to exercise its control function.

The disciplinary file claimed may contain, or may be derived from, different or complementary information to that provided by the Department to the deputy in response to the parliamentary question formulated by his parliamentary group, consisting of the initiation of a prior information by the Directorate of Internal Affairs at the request of the Police Prefecture once the news given by a means of communication became known, which led to the opening of a disciplinary file against a member of the police force and the imposition of a penalty. It cannot be ruled out that this other information may be relevant to the control purpose of the Administration that corresponds to the deputy (it could, for example, allow us to evaluate what actions the Department undertook in this regard, how they developed and which be the result
specific).

However, it must be borne in mind that the disclosure of the information that may include this type of file in such a way that the sanctioned person is identified or identifiable may cause serious damage to their privacy, particularly in view of the nature of the facts investigated and sanctioned, as well as affecting their social and professional image, even their personal safety.

Taking into account the intended purpose of control with access, which must be framed in the parliamentary control over the Department's action in the face of facts that affect the police force's procedure, it is not sufficiently justified what relevance for the control of the performance of
Once the Administration learns of the facts mentioned by a media outlet, it may have the requested information available so that the person affected can be identified.

v

Similar considerations can be made regarding the identification of those people who have given a statement in the course of the same disciplinary procedure - or of the previous information, in the case of having joined the procedure -, and who appear in the file.

The deputy's access to this information requires a reasoned weighting between the public interest in its disclosure and the rights of the affected persons in accordance with article 24.2 of the LTC.

In this sense, it must be borne in mind that the reserved nature of this type of procedure means that these people who declare or provide information about the facts under investigation do so in the confidence that, without prejudice to the access necessary to guarantee the right of defense of the persons responsible, their identity is preserved. especially

in this case, in which, according to the information available, part or most of these people work or have worked in information units of the police force, so they may require a reinforced need for reservation respect their identity.

But, beyond that, it is also not appreciated what relevance, for the exercise of the function of control over the management of the Department following the events that occurred on the part of the deputy, it would have have the specific identity of the persons declaring.

On the other hand, as indicated in the report issued in relation to the claim presented, the disciplinary file also contains data relating to the participants in an opposition contest to be promoted to the corporal category. The reason, maintains the Department, is that this fact justified the temporary suspension of the execution of the sanction imposed on the agent.

The knowledge of these circumstances, that is the existence of this competition and of the temporary suspension of the execution of the sanction by the deputy may be relevant to the effects of control of the Department's action. The delivery of this type of information, as it does not contain personal data, would not pose any problems from the point of view of data protection.

Beyond this, it would not be justified to give the deputy any other type of information about the selection process that would allow the sanctioned agent or the other participants to be identified in the disciplinary file to be identified, given that their knowledge would not be relevant in attention to the intended purpose of the access.

The achievement of the objective of parliamentary control of the actions of the Administration in the present case could also be achieved without sacrificing the right to data protection of the agent affected by the disciplinary procedure or of the rest of the people affected by access, through the delivery of the file in question in an anonymized manner. An option expressly foreseen both in the transparency legislation (article 15.4 LT and article 70.5 of Decree 8/2021, of February 9, on transparency and the right of access to public information) and in the RPC (article 5.2 ter), in order to make effective the right of access of the deputies.

For the purposes of anonymizing the file, it must be agreed that, in order for it to be considered sufficient, in terms of data protection legislation, it must be guaranteed that the information provided cannot be linked to a person physical identified or identifiable. Thus, anonymization would require the elimination of all information that could allow the identification of the person or persons affected, taking into account not only the information contained in the
documents that make it up but the data that can be obtained by other means, objectively assessing whether or not there is a real risk of re-identifying the affected people without making disproportionate efforts.

Point out, with attention to the context in which we find ourselves, that the data relating to the professional identification number (TIP) constitutes for all purposes personal data, given that it also allows
the identification of the person, even though, for a third party, it may require a greater effort to identify them by their TIP than by their first and last names. Therefore, it is a fact that should not be included in the information that is given to the deputy.

For the information that is available, the complaining deputy agrees that the file in question be provided anonymously. However, he also states that "the non-inclusion of TIPS collides head-on with the task of parliamentary control that we are obliged to exercise, already

which prevents us from being able to verify and assess that the appropriate procedures have been followed in this file".

When the anonymization of the information does not allow the intended purpose to be achieved, there is also the possibility of providing said information prior to pseudonymization of the data, which, in terms of article 4.5 of the RGPD, consists in treating the personal data in a way that the information to which you have access can no longer be attributed to the data holder without using additional information, provided that this additional information is recorded separately and is subject to technical and organizational measures aimed at ensuring that the personal data are not attribute to an identified or identifiable natural person.

Therefore, in a case like the one proposed, the option of delivering the requested file after data pseudonymization could be considered, this is by replacing the name and surname or any other identifying data (such as the TIP) of the people affected by a code, so that if there is no additional information, known only to the person who carried out the pseudonymisation, which allows establishing a link, it is not possible to know who this code corresponds to.

Facilitating the file prior to pseudonymisation of the data would facilitate the deputy's control of the Department's action in the case examined (it would make it possible to know if the action of the Internal Affairs Division conforms to the law, if the timely procedures, how many people have been involved, etc.) without sacrificing the right to data protection of the sanctioned agent and the rest of the people affected.

This pseudonymization of data should not include the merely identifying information of public employees who, by reason of their functions, have intervened in the disciplinary procedure, unless there are specific circumstances that justify the prevalence of the right to the protection of the person's data or affected persons (article 24.1 LTC). However, in the case of members of a police force, their identification should in any case be carried out using the assigned TIP (article 70.3 RLTC).

All this, without prejudice to the application of any other limit other than the protection of personal data that may limit the deputy's access to the requested information.

conclusion

From the point of view of data protection, the deputy's access to the requested disciplinary file can be effected after pseudonymisation of the personal data contained therein.
This, without prejudice to the possible application of other limits that may limit access.

Barcelona, November 10, 2021