CNS 42/2020

Opinion in relation to the inquiry made by an entity in relation to the processing of personal data contained in the investigation actions of the Office, to which deputies of the Parliament of Catalonia request access to the protection of the right of access recognized in article 6 et seq. of the Regulation of the Parliament of Catalonia.

Background

A query from the director of an entity is presented to the Catalan Data Protection Authority in relation to the processing of personal data contained in the research actions it carries out, to which deputies and deputies of the Parliament of Catalonia under the protection of the right of access recognized in article 6 et seq. of the Regulations of the Parliament of Catalonia.

The inquiry states that the entity has received several requests for access to public information from members of the Parliament of Catalonia, relating to research actions carried out by the entity. Once the aforementioned requests have been analyzed, the entity wants to know the opinion of the Authority regarding the following issues:

"- If, in order to satisfy the right of access, it would be in accordance with the Law to allow direct access to the proceedings at the headquarters (...) (only a view of the proceedings without obtaining a copy), without anonymization of personal data that contain the actions and with the commitment of confidentiality and the preventions referred to, for example, in art. 15.5 of Law 19/2013, of December 9, on transparency, access to public information and good governance or art. 5.1 f) of Regulation (EU) no. 2016/679 of the European Parliament and of the Council, of April 27, 2016, relating to the protection of natural persons with regard to the processing of personal data and the free movement of such data;

What should be the security measures that should be applied by the person responsible for the processing of personal data in relation to this possible view of the investigative actions in person at the headquarters of the Office;

In relation to the previous inquiries, it should be borne in mind that some of the actions could have led to judicial actions of a criminal nature, or in eventual sanctioning or, more specifically, disciplinary procedures, instructed by the competent administrations;

- Application of restrictions on the right of access in relation to complaints submitted to (...), in order to protect the identity of the person making the alert; at this point (...) considers that this personal data should enjoy special protection in accordance with the principles established by EU Directive 2019/1937, of the European Parliament and of the Council, of October 23, 2019 , regarding the protection of people who report violations of Union Law and our rules of action and internal regime, especially given that we understand that access to the complaint would not seem necessary to satisfy the purpose of the right to 'access;

- Regarding the delivery of copies of documentation corresponding to these investigative actions (after or before the hearing to which we have referred) if the protection of personal data that should be done ("anonymization") would be the same that what would be done in relation to any other access to public information of citizens, or the deputies have a wider right of access specifically from the point of view of data protection regulations, given their function and, in this specific case, given the affiliation (...) to the Parliament of Catalonia."

Having analyzed the query, which is not accompanied by other documentation, in accordance with the report of the Legal Counsel I issue the following opinion:

Legal Foundations

I

(...)
II

First of all, in order to focus the query raised from the point of view of data protection regulations, it must be taken into account that, in accordance with Regulation (EU) 2016/679, of the Parliament and of the European Council, of April 27, 2016, General Data Protection Regulation (hereinafter, RGPD) any processing of personal data, understood as *"any operation or set of operations carried out on personal data or sets of personal data, either by automated procedures or no, 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." (article* 4.2 RGPD), has submitted to the principles and guarantees established by that Regulation.

The RGPD defines personal data as: *"all information about an identified or identifiable natural person (the "data subject"); Any person whose identity can be determined, directly or indirectly, in particular by means of an identifier, such as a number, an identification number, location data, an online identifier or one or more elements of identity, shall be considered an identifiable physical person physical, physiological, genetic, psychological, economic, cultural or social of said person;* (Article 4.1 GDPR).

Article 5.1.a) of the RGPD establishes that all processing of personal data must be lawful, fair and transparent in relation to the interested party (principle of lawfulness, loyalty and transparency).

In order for a treatment to be lawful, it is necessary to have, at least, a legal basis of those provided for in article 6.1 of the RGPD that legitimizes this treatment, either the consent of the person affected, or any of the other circumstances which provides for the same precept. In the field of public administrations, the legal bases provided for in letters c) and e) of article 6.1 of the RGPD are of particular interest, according to which the treatment will be lawful when it is necessary for the fulfillment of a legal obligation applicable to the person responsible for the treatment (letter c), or when the treatment is necessary for the fulfillment of a public interest or in the exercise of public powers conferred on the person responsible for the treatment (letter e).

However, as can be seen from Article 6.3 of the RGPD, the legal basis for the treatment indicated in both cases must be established by European Union Law or by the law of the Member States that applies to the person responsible for treatment. The referral to the legitimate basis established in accordance with the internal law of the member states requires, in the case of the Spanish State, in accordance with article 53 of the Spanish Constitution, that the rule of development, to be about a fundamental right, has the status of law.

In this sense, article 8 of Organic Law 3/2018, of December 5, on Protection of Personal Data and guarantee of digital rights establishes the need for the enabling rule to have the status of law.

In accordance with article 55 of the EAC, the Parliament represents the people of Catalonia, and *"exercises legislative power, approves the budgets of the Generalitat and* ***controls and promotes political and government action."***

The fifth Additional Provision of Law 19/2014, of December 29, on transparency, access to public information and good governance (hereafter, LTC) 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 Parliament must determine the necessary adaptations derived from nature

institutional of the Parliament, which in no case can lead to a lower guarantee regime than that established by this law.

4. Parliament must establish a procedure to consolidate the laws that are the subject of partial modifications with the aim of simplifying the system, improving its quality and contributing to the guarantee of legal security. The consolidation procedure must give rise to texts with legal value that replace and repeal the laws subject to consolidation."

Article 6 of the Regulations of the Parliament of Catalonia (hereafter RPC) provides the following:

"1. Deputies, in the exercise of their function, have the right to access information, and obtain a copy, from the Administration of the Generalitat, from the bodies, companies and entities that depend on them and from the institutions and the 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 required authorities or administration must provide the deputies, preferably electronically, or on paper, with the requested information.

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."

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

The administrative scope on which the right of access of the deputies of the Parliament of Catalonia is projected is determined by article 6 RPC, and covers the information of *"the Administration of the Generalitat, the bodies, the companies and the entities that depend on it and the institutions and bodies of the Generalitat that act with functional independence or with a special autonomy recognized by law".*

The information on the actions carried out by the entity, as a public law entity with its own legal personality and full capacity to act attached to the Parliament of Catalonia, which aims to prevent and investigate possible specific cases of use or illegal allocation of public funds or any other irregular use resulting from conduct that involves conflicts of interest or the use for private benefit of information derived from the duties of personnel in the service of the public sector (article 1 of Law 14 /2008, of November 5), is information that remains

subject to the regime of access recognized to deputies by the aforementioned article 6 of the RPC.

Therefore, from the perspective of data protection regulations, make it easier for deputies
the exercise of the right of access to the information available to the entity is considered a lawful treatment in accordance with article 6.1.e) of the RGPD (treatment necessary for the fulfillment of a public interest or in the exercise of public powers conferred on the data controller) in relation to article 6 of the RPC.

However, this treatment must be subject to the regime of regulated access to the RPC and the principles and guarantees of the RGPD.

III

The first question formulated by the ORGANIZATION raises whether, in order to satisfy the right of access of the deputies, it would be legal to allow direct access to proceedings at the ORGANIZATION headquarters with a view of the actions, without providing a copy, but without the anonymization of the personal data that they contain with the commitment of confidentiality on the part of these respect to the information to which they have access.

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 *"citizens have 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, the 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 regulation of this right in the Regulations of the Parliament of Catalonia is foreseen, as explained, in article 6 which provides that deputies, in the exercise of their duties, have the right to access information , and to obtain a copy, from the Administration of the Generalitat, the bodies, companies and entities that depend on them and from the institutions and bodies of the Generalitat that act with functional independence or with a special autonomy recognized by law.

This right can also be exercised by consulting the information at the offices of the required administration in accordance with the provisions of article 10 of the RPC which under the title *"Right of direct access to information"* regulates the possibility for deputies to consult in person the information and documentation requested in exercise of the right of access to information.
Thus, this article 10 establishes the following:

> *"1. If the deputy wants to go to the administration offices to consult in person the information and documentation requested in the exercise of the right regulated by article 6, he can do so accompanied, at the most, by two duly accredited advisors.*
>
> *2. The personnel who provide assistance to a parliamentary group or a member of Parliament in proceedings before the Administration of the Generalitat and the other bodies and entities referred to in article 6 must be duly accredited by the General Secretariat of Parliament."*

According to this legal configuration, the right of access to the information of the deputies is an individual right that can be exercised by all the members of the Chamber by directly requesting this information or through the President of the Chamber, and includes the answer to the questions , the copying of requested documents or the direct consultation of the information in the offices of the Administration with the assistance of up to two advisers accredited by the General Secretariat of the Parliament.

However, article 7 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."*

Article 7.1 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."*

The consideration of this right as preferred by article 7.2 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 the deputies have a strengthened position compared to that which citizens in general can have. Consequently, the limitations of the right of access will have to be interpreted even more restrictively.

Therefore, although the limits to access to information are the same in the regime of access to information for members of Parliament regulated in the Rules of the Chamber and in the general regime of access to information of all the citizenship established in the transparency legislation, it is necessary to weigh them according to what the jurisprudence has called the *"essential added plus"* who must have access to the information of the deputies on the information available to any citizen, so that they can exercise their representative function (STS of June 15, 2015).

Consequently, when the information to which the deputies request access (either by traveling to the headquarters of the required administration and accessing the documentation in person or by sending copies of the proceedings) contains personal data, the eventual collision between the right of deputies to access information and the right to the protection of personal data, must be resolved in accordance with the criteria provided for in articles 23 and 24 of the LTC and with the principles of the data protection regulations taking into consideration the strengthened position of parliamentarians or *"essential addition".*

IV

In the consultation, it is stated that some of the actions to which access is requested could have resulted in judicial actions of a criminal nature, or in eventual sanctioning or, more specifically, disciplinary procedures, instructed by the competent administrations.
To the extent that the actions of THE ENTITY have as their object the investigation of alleged irregular facts attributable to certain persons, whose conduct could constitute criminal or administrative offences, the information referred to these persons is deserving of special protection.

According to article 23 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, the trade union affiliation, 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, unless the affected party expressly consents to it by means of a written document that must accompany the request."*

Along the same line, article 15 of the 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 15.5 of the LT when the information to which the deputies want to access contains special categories of data in the opinion CNS 16/2019 which can be consulted on the website www.apdcat.cat. 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 require in any case, to have the prior consent of the person affected.

(...)

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 information of citizens referred to in this article, although and that access cannot be ruled out

deputies to certain information referred to in these articles, always with restrictive criteria, in particular when it refers to public positions that are subject to the control of the Parliament, which may be essential for the exercise of the functions attributed to the Parliament ."

Consequently, in the face of a request for access by deputies, to the offices of THE ENTITY, to information on procedures that could have resulted in judicial proceedings of a criminal nature or in eventual sanctioning or disciplinary procedures instructed by the competent administrations, given that the information would contain categories of data protected by the transparency regulations, access to this information would have to be limited except for the analysis of the specific case -given the preferential nature of the right of access of the deputies-, the information to which access may be considered essential to exercise its control function.

It should be borne in mind that the information that can be included in these types of files can have strong implications for the lives of the people affected. Apart from the nature of this type of information, and the consequences that its disclosure may have from the point of view of the private life or the social and professional image of the people affected, it is also necessary to take into account that this is information that at this stage may not be sufficiently verified (at this stage the judicial or administrative procedure to demand responsibilities has not yet been processed) and it is also possible that they are being carried out or should be carried out carry out investigations by the judicial police or by the competent body.

Taking this into account, and as it follows from Article 7.2 RPC, in the event that these circumstances require it, the delivery of the requested information in an anonymized way could be sufficient (for example it may allow to evaluate the activity of the entity, the types of files, the resources used, the outcome of the procedures, etc.) this option should be chosen.

For the purposes of proceeding with the anonymization of the information, it must be agreed that, in order for it to be considered sufficient, in terms of the data protection legislation, it is necessary to guarantee that the information provided cannot relate- with an identified or identifiable natural person. Thus, anonymization would require the elimination of all the information that could allow the identification of the person or persons affected, taking into account not only the information contained in the document but also the data that can be obtained by other means, assessing objectively whether or not there is a real risk of re-identifying the affected persons without making disproportionate efforts.

There is also the possibility of providing information prior to pseudonymisation of the data, which in terms of article 4.5 of the RGPD, consists in treating personal data in such a way that the information to which access is no longer 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 is not attributed to an identified or identifiable natural person.

If anonymized or pseudonymized information is not sufficient to be able to carry out the control activity, because it is necessary to identify the specific people affected (for example because the requesting deputies need to identify the people with public positions under their scope of control that have been investigated by the entity), it is necessary to take into account the possibility of partial access, also provided for by article 7.2 RPC. Thus, it cannot be ruled out that, depending on the

circumstances, it may be justified to identify the affected persons by revealing certain data regarding concluded procedures, such as the result of the procedure instructed by the entity, but on the other hand, generalized access to all the information that may be contained in the instructed files does not seem a priori justified .

v

In the requested documentation, in addition to specially protected data, it is also foreseeable that other personal information will be included. Regarding this, the provisions of article 24 of the LTC must be applied:

"1. Access to public information must be given if it is information directly related to the organization, operation or public activity of the Administration that contains merely identifying personal data unless, exceptionally, in the specific case it has to prevail over the protection of personal data or other constitutionally protected rights.

2. If it is other information that contains personal data not included in article 23, access to the information can be given, with the previous reasoned weighting of the public interest in the disclosure and the rights of the people affected. To carry out this weighting, the following circumstances must be taken into account, among others:

a) The elapsed time.

b) The purpose of the access, especially if it has a historical, statistical or scientific purpose, and the guarantees offered.

c) The fact that it is data relating to minors.

d) The fact that it may affect the safety of people.

3. Requests for access to public information that refer only to the applicant's personal data must be resolved in accordance with the regulation of the right of access established by the data protection legislation staff."

According to article 24.1 of the LTC, access to public information must be given if it is of information directly related to the organization, operation or public activity of the Administration that contains merely identifying personal data unless, exceptionally, in the specific case the protection of personal data or other rights must prevail constitutionally protected.

In this case, the identification data (name and surname and position) of the public employees who appear identified for having intervened in the exercise of their functions in the actions subject to investigation, as well as the staff of the entity that has intervened, would be included in investigations. In principle, from the perspective of data protection regulations, there should be no impediment to allowing access to said information, unless the personal situation of any of these people can justify the limitation.

Apart from these cases, article 24.2 establishes that access to information can be given with prior weighting reasoned between the public interest in the disclosure of the information and the rights of the persons affected. It is, in short, to see in each case which personal information is affected, and to apply the guidelines and criteria provided for in the transparency legislation and the principles and guarantees provided for in the data protection regulations. All this bearing in mind that the right of access to the information of the deputies, as has been explained, is inserted within the parliamentary functions, singularly within the functions of impulse and control of the Government and the administration. This function of parliamentary control constitutes an essential function, recognized in the EC and the Statute of Autonomy and is closely related to the parliamentary system of government and to the democratic system of control of the activities of the public authorities by the elected members as to representatives of the citizens.

Finally, in this analysis and weighting, it will also be necessary to apply, among others, the principle of data minimization (Article 5.1 d) RGPD) which requires that the data subjected to treatment are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

In short, the review of the file by the deputies must be carried out in such a way that access is only given to that information which, in the analysis of each specific case in accordance with the criteria set out, is necessary to exercise this control function (so, for example, in general data can be considered unnecessary for the purpose for which they are processed the ID number, postal or electronic address, telephone number, etc. of the persons that may be included in the requested information).

These considerations would apply both to direct access to the files (first question of the consultation) and to obtaining copies (third question).

VI

The second issue raised by the entity refers to the protection of the identity of the "alerting" person. The entity considers *"that these personal data should enjoy special protection in accordance with the principles established by EU Directive 2019/1937, of the European Parliament and of the Council, of October 23, 2019, relating to the protection of people who report violations of Union Law and our rules of action and internal regime, especially given that we understand that access to the complaint would not seem necessary to satisfy the purpose of the right of access;*

With respect to the protection of the identity of *"whistleblowers"* or people who bring to the notice of the entity the facts that may lead to the initiation of its actions, it is necessary to take into consideration what is established in article 16.3 of Law 14/2008 according to which:

> *"3. Anyone can contact the Anti-Fraud Office to report suspected acts of corruption, fraudulent practices or illegal conduct that affects the general interests or the management of public funds. In this case, receipt of the received letter or communication must be acknowledged.* ***The reporting person can request that confidentiality be kept about the***

his identity, and the staff of the Antifraud Office is obliged to maintain it, except in the event that he receives a judicial request."

This precept obliges the entity to maintain the confidentiality of the reporting person, if the latter so states, except in cases where there is a judicial requirement.

Outside of these cases, when there is no express manifestation of the will of the reporting person regarding access to their identity, in order to determine the provenance of facilitating access to their identity, it is considered appropriate to transfer the access request to them, making them aware of the possibility that they have in accordance with article 16.3 of Law 14/2008 to express their interest in maintaining the confidentiality of their identity. If the person shows his opposition to the access, this should be limited under the protection of the specific rule mentioned.

In the consultation, reference is made to the special protection of the whistleblower by application of the principles contained in EU Directive 2019/1937, of the European Parliament and of the Council, of October 23, 2019, relating to the protection of persons who report on violations of Union Law.

With regard to this matter, it will be necessary to comply with the regulations for the transposition of the aforementioned Directive, which entered into force on December 16, 2019, - twenty days after its publication in the Official Journal of the European Union - but that it has not been transposed to our internal regulations.

It must be taken into consideration that the legislator is still within the deadline for its transposition (in accordance with its article 26, the member states have until December 17, 2021 to put into force the legal, regulatory and administrative provisions necessary to comply with the established therein, and until the 17 of December 2023 to put into force the legal, regulatory and administrative provisions necessary to comply with the obligation to establish internal reporting channels for legal entities in the private sector that have 50 to 249 employees).

It should be remembered that the doctrine of the Court of Justice of the European Union regarding the direct applicability or direct effect of Community directives requires that, in addition to having passed the transposition period without having occurred or having incorrectly carried out said transposition, its provisions are clear and precise, that is to say, it must contain an effectively imperative right or obligation and, in addition, the rule must be complete and legally perfect, that is to say it must not need no complementary measure for its application and, in the case of need, the national authorities should not have any discretionary power of appreciation. Therefore, an application of the aforementioned directive to the case at hand must be ruled out.

In this sense, the recent judgment of the Superior Court of Justice of the Valencian Community of June 4, 2020 (Sentence no. 198/2020) is pronounced regarding an appeal on the limitation of access of regional parliamentarians to documents or files that open in bodies not dependent on the executive, as is the case in the Valencian community of the Valencian Antifraud Agency, and, specifically, with respect to the application of Directive 21019/1937 with regard to the complainant's confidentiality, has highlighted the following: I

(...)

Already in the jurisdiction ex novo the defendant invokes the protection of the confidentiality of the complainant; allegation that also appears in the prosecutor's conclusions, based on article 16 of Directive (EU) 2019/1937 infractions of Union law.
(...)

So the time has not expired to carry out the transposition on the part of the different regulatory powers (Las Corts, in our case) and bearing in mind that, regardless of the expansive vision that can be reached in the future as suggested by certain scientific doctrine, the scope of application of the Directive is limited to infractions that affect common policies or European Union law in certain areas, so that it is far from regulating situations like the one in the present case, given the material areas and personal application articles 2 and 4. (FD octavo)"

Therefore, the aforementioned Directive does not constitute a rule applicable to the case at hand, as long as it is not transposed, or cannot have, in some of its provisions, a direct effect.

However, it must be taken into account that article 24 of Law 3/2018, of December 5, on the protection of personal data and guarantee of digital rights (LOPDGDD), regulates the information systems for internal complaints in the terms next:

1. It will be lawful to create and maintain information systems through which a private law entity can be made aware, including anonymously, of the commission within it or the performance of third parties who contract with it, of acts or conduct that could be contrary to the general or sectoral regulations that were applicable. Employees and third parties must be informed about the existence of these information systems.

2. Access to the data contained in these systems will be limited exclusively to those, whether or not affiliated with the entity, who carry out internal control and compliance functions, or to those in charge of processing that are eventually designated for that purpose. However, its access by other persons, or even its communication to third parties, will be permitted when it is necessary for the adoption of disciplinary measures or for the processing of the judicial proceedings that, in their case, proceed.
Without prejudice to the notification to the competent authority of facts constituting a criminal or administrative offence, only when the adoption of disciplinary measures against an employee could proceed, said access will be granted to personnel with functions of management and control of human resources.

3. The necessary measures must be taken to preserve the identity and guarantee the confidentiality of the data corresponding to the persons affected by the information provided, especially that of the person who had brought the facts to the knowledge of the entity, in case it had been identified

4. The data of the person making the communication and of the employees and third parties must be kept in the reporting system only for the time necessary to decide on the origin of starting an investigation on the facts reported.

In any case, after three months have passed since the introduction of the data, it must be deleted from the reporting system, unless the purpose of the conservation is to leave evidence of the operation of the crime prevention model by the legal entity. Complaints that have not been acted upon may only be recorded anonymously, without the blocking obligation provided for in article 32 of this organic law being applicable.

After the period mentioned in the previous paragraph, the data may continue to be processed, by the body to which it corresponds, in accordance with section 2 of this article, the investigation of the reported facts, not being kept in the internal reporting information system itself.

5. The principles of the previous sections will be applicable to the internal reporting systems that could be created in the Public Administrations.

It could be the case that, among the investigative actions of the Office to which deputies of the Parliament of Catalonia have requested access, there were some that had their origin in internal complaints submitted to one of the bodies of its scope of action
through an internal complaints system regulated in article 24 LOPDGDD.

In these cases, the receiving body of the internal complaint that chooses to request the entity's intervention - prior to other jurisdictional or disciplinary actions - would be obliged, by application of the third section of article 24 LOPDDD, to preserve the identity and guarantee the confidentiality of the reporting person (article 24.3 LOPGDD). In any case, if as a result of the investigation actions this entity could have come to know the identity of the person making the complaint, the obligation to preserve the identity of the complainant provided for in the LOPDGDD would also be extended to the actions of the entity, which should take the
appropriate measures to guarantee it against the access of the deputies (either in person or by sending a copy) to these investigation actions of the entity.

Conclusions

Members of Parliament can exercise the right of access to the information held by the entity by virtue of the right recognized by the RPC, either by copying requested documents, or directly consulting the information in the offices of the Administration with the assistance of up to two advisers accredited by the General Secretariat of the Parliament. Despite the preferential nature of this right, the limits provided for in the regulations governing the right of access to public information are applicable.

When the information contains data relating to infringements or criminal or administrative sanctions (or other data provided for in Article 23 LTC), access to this information must in principle be limited. When it is essential to identify the affected persons, with respect to the completed procedures, information can be provided on the outcome of the procedures processed by the entity, but access to the entire file must be avoided.

As for the rest of the information, access can be given, although under the principle of minimization it is necessary to exclude those data that are unnecessary for the control function carried out by the deputies, of in accordance with what is set out in Legal Basis V.

The identification of the person making the complaint or who brings the facts that give rise to their actions to the attention of the entity must be preserved if they state so, either in the complaint or later in the hearing procedure granted to them , unless there is a judicial requirement.

Barcelona, December 17, 2020