CNS 39/2021

Opinion in relation to the consultation of a City Council in relation to access to the local team of a City Council official, for the purposes of being able to access City Council information

A letter from a City Council is presented to the Catalan Data Protection Authority, in which an Opinion is requested from this Authority in relation to the possibility of accessing the local equipment used by a City Council official, which is on leave, to be able to access information owned by the City Council, through its IT department.

Having analyzed the request, which is not accompanied by more information, in view of the current applicable regulations and in accordance with the report of the Legal Counsel, the following is ruled.

I

(...)

II

The query refers to the possibility of access to the local team used by a City Council official, who is on leave, for the purposes of being able to access documentation from the City Council's Department of Citizen Participation. The consultation explains that the official "is the only user who centralizes this Office, and therefore creates and saves the documentation." According to the consultation, not being able to access this information paralyzes and affects the development of the City Council's actions, and adds that the official in question has a disciplinary matter with the City Council, which is still pending resolution.

The consultation adds that City Council officials received data protection training and were explained the City Council's security protocol (among others, that personal topics are not allowed in the city's work tools 'Council, that the workers have been notified of the possibility of access to all control tools owned by the Council, and that it is foreseen that all documentation must be kept in enabled spaces).

At this point, it should be noted that, beyond the fact that the references made in the consultation to some sections of said protocol serve to frame the hypothesis raised, the purpose of this report is not to make an assessment or validation of the adequacy of the City Council protocol to the data protection regulations.

Having said that, the query asks "if we can access the local team in which a City Council official carries out his functions, for the purposes of being able to access information owned by the City Council, through the City Council's IT Department, for the following purposes :

A) Put all the documentation that may exist from the aforementioned Council in the spaces intended for the purpose B) Guarantee the integrity of the documentation given that it is not in a space where backup copies are made C) Corroborate if the measures are being breached of security of the City Council, a possibility that is communicated and accepted by the officials D) Unblock the paralysis of the Council, understanding that it is a proportionate measure and the good to be protected is greater than what could be harmed. That is to say, the development of a Council, - general interest and multiple affected - is more important than access to the team of a civil servant, where there could, and we emphasize "could", exist personal information, which in no case, we want access E) That any action is scrupulous with the possibility of finding a document of a private nature, even though personal topics are prohibited in the work tools, taking care and avoiding in this case, any opening and access to this content F) That the 'access would be made by the external - IT Systems Administrator G) If they understand that this action must be communicated to the affected person, in case they consider that access can be made, although the query is made from the perspective that the affected person does not give his consent."

According to the consultation, this is considered "from the perspective that the affected person does not give his consent." Taking this into account, starting from the premise that in the case raised the City Council would not have the employee's consent, it will be necessary to see if any of the legal bases of article 6.1 RGPD, which allow the processing of data to be considered lawful, and under what conditions

III

According to article 87 of the LOPDGDD:

> **"1. Workers and public employees have the right to the protection of their privacy in the use of digital devices made available to them by their employer.**
>
> **2. The employer will be able to access the content derived from the use of digital media provided to the workers for the sole purpose of monitoring compliance with labor or statutory obligations and guaranteeing the integrity of said devices.**
>
> **3. Employers must establish criteria for the use of digital devices respecting in any case the minimum standards of protection of their privacy in accordance with social uses and constitutionally and legally recognized rights. Workers' representatives must participate in its preparation.**
>
> **The access by the employer to the content of digital devices with respect to those that have admitted their use for private purposes will require that the authorized uses be precisely specified and that guarantees be established to preserve the privacy of the workers, such as, where appropriate, the determination of the periods in which the devices may be used for private purposes.**
>
> **Workers must be informed of the use criteria referred to in this section."**

It is also necessary to take into account several provisions of the labor regulations, in relation to the lawfulness of the control measures by the employer - in this case, a Public Administration -, the compliance by the workers, of the their work obligations.

In particular, article 52 of the Basic Statute of the Public Employee (EBEP), according to which: "Public employees must diligently carry out the tasks assigned to them and look after the general interests subject to and observing the Constitution and the rest of the legal system (...)", and article 20.3 of the Workers' Statute (ET), according to which: "The employer may adopt the surveillance and control measures it deems most appropriate to verify compliance by the worker of his obligations and labor duties, keeping in his adoption and application the consideration due to his dignity (...)".

From the perspective of the data protection regulations, as can be seen from article 87 of the LOPDGDD, the purposes for which it would be lawful to monitor the equipment that the employer makes available to the workers, would be, d on the one hand, the control of the fulfillment of the worker's labor obligations (in connection with the provisions of the labor regulations), and on the other, that of guaranteeing the integrity of the devices used by the workers to carry out their duties .

In the case examined, and according to the available information, the City Council (responsible for the processing pursuant to art. 4.7 RGPD), points out that the main purpose of access to the equipment assigned to the official who is on leave would be the to ensure the continuity of the work carried out by the City Council since, according to the City Council, the documentation stored in the local equipment used by the worker would be "essential to be able to continue with the activity carried out by the Council ").

We note that the "purposes" referred to in questions A) and D) of the consultation ("Put all the documentation that may exist from the Council in the spaces intended for the purpose" and "Unblock the paralysis of the Council (...)"), given the information available, it seems that they refer to or are related to this general purpose of ensuring the fulfillment of the functions carried out by the Council's Office.

To this it should be added that question B) "Guarantee the integrity of the documentation given that it is not in a space where backup copies are made", according to the information available, would also refer to the purpose of accessing the team in question in order to protect the documentation of the Council and therefore, to ensure the work carried out by the City Council.

As the jurisprudence has admitted (for example, the STC 61/2021, to which we refer), the employer can establish controls on the use of the tools he makes available to the workers. Particularly relevant is the STEDH, Barbulescu case, of September 5, 2017, in which the TEHDH establishes certain elements that should be applied in this context. In summary, the ECtHR refers to the information that must be given to workers regarding the measures that the employer can take to monitor these tools, in particular, the workers' communications; what is the scope of supervision, or if the employer has assessed the existence of less intrusive control measures for workers, among others (section 210 of the STEDH of September 5, 2017, to which we refer).

According to the query, the City Council's protocol refers to the fact that the person in charge of the treatment "also informs the users that possible controls will be carried out

(PC content, email, internet connections, servers and contracted software) (...).”

We note that this Authority has issued Recommendation 1/2013, on the use of e-mail in the workplace (available on the website www.apdcat.cat), in which different considerations are made that are of particular interest in this case, and to which we refer.

In section III of the Recommendation, referring to access to e-mail by the company, it is also agreed that the means and scope of the control must be proportionate to the purpose pursued, and 'identify the objectives that could justify access, in this case, to the equipment or other devices that the employer makes available to the workers, in order to access the documentation of the Regional Office.

Specifically, the Recommendation identifies the possibility of access in order to guarantee the continuity of the activity in the absence of the working person (vacation, illness, etc.), bearing in mind that the absence of a worker, especially if it is of long duration, it may lead to problems for the normal continuity of the activity, if it is not possible to access certain information that, in the case at hand, would be found in the equipment available to the worker in a situation of come down Especially taking into account that, according to the consultation, this worker is "the only user who centralizes the information of the Council", which would have caused, according to the consultation, the paralysis of the functions carried out by it.

We also add that, as shown in section III of the Recommendation - and given that it is not known whether the City Council's protocol has provided for it - it is recommended that, when the intervention is justified for this purpose of ensuring the continuity of work activity, "it is convenient, if possible, to plan the measures that will be adopted to guarantee continuity during the absence" and, if this is not possible, the worker's superior body should "evaluate in a motivated way the need for the intervention for the continuity of the service."

In application of the principle of proactive responsibility (art. 5.2 RGPD), the person responsible, in this case, the City Council, must answer for compliance with the principles of data protection, and for this reason, for the purposes they are concerned, it would not be sufficient to ·bequeath a purpose for access that in general terms may be lawful, but it will be necessary to motivate it based on the circumstances of each case.

In this case, the consultation states that the documentation deposited in the local team of the worker who is on leave, is essential to be able to continue with the activity carried out by the Regional Office, and that not being able to access the information of the Council paralyzes and affects the development of the actions carried out in the City Council, so that, always according to the consultation, since the employee's leave it has not been possible to continue with the normal activity of the Council.

Point out, in any case, that in general it would be necessary for the City Council to assess the risks that for the information of the City Council it must deal with being stored locally on equipment for which there is no backup copy. The guarantee of the integrity and availability of the information would require the information to be stored using systems that allow periodic backup copies to be made periodically, which should be guarded by the City Council.

Taking into account all the above, and given the information available, in principle it could be considered that the treatment subject to consultation could be lawful for the fulfillment of this purpose (to guarantee the continuity of the work of the Council in the absence of the worker who is on leave), for the purposes of the provisions of article 6.1,

section e) of the RGPD, in connection with the regulatory provisions we have mentioned (labour regulations and art. 87 LOPDGDD). This, as long as it is necessary to ensure the normal functioning of the work carried out by the Town Hall - as it seems to be the case examined, given the information available -.

IV

Still in relation to the lawfulness of access, question C) asks if access to the worker's equipment could be justified, to "Corroborate if the City Council's security measures are being breached, a possibility that has been communicated and accepted by officials".

It seems, from the information available, that in this case the City Council considers whether access is not already based on a purpose of guaranteeing the continuity of the activity of the Council - an issue already discussed - but to verify non-compliance - on the part of the worker - of the security measures that, based on the information available, the City Council could have foreseen in the corresponding protocol.

It should be remembered that, according to the consultation, in the case raised the civil servant in question "has a disciplinary matter with the City Council, still pending resolution."

From the available information, it is not known whether the disciplinary matter referred to by the City Council has any connection with the possible misuse of the media worker (computer equipment, e-mail, etc.), which the City Council would have made available to him, or if access to the equipment, object of inquiry, may be relevant or necessary for these purposes, and in measure

In view of the information available, this report cannot determine whether the possible indications of misuse or "possible breach of security measures" by the worker, which the City Council may have, would be sufficient to justify or consider the intervention of the worker's team lawful or proportionate in the specific case being analyzed.

Having made this consideration, and in general terms, it is worth remembering that, according to article 87.2 LOPDGDD, it is considered lawful for the employer to access content derived from the use of the media that he makes available to his employees, in order to "guarantee the integrity of these devices".

To the extent, then, that the purpose intended by the City Council is to detect possible breaches of the security measures that it has previously made known to the workers through the protocol or the training that would have been given to the workers and, in short, guarantee the appropriate use of the equipment made available to the worker and the integrity and security of the information and documentation contained therein, in principle it could be understood that the access responds to a purpose provided for in the regulation that, therefore, can be lawful.

In this sense, as this Authority has agreed in Recommendation 1/2013, access based on the purpose of verifying possible misuse of the equipment that the City Council makes available to workers) must be provided to the type of risk that may arise from misuse of the equipment or the worker's email account, in the terms set out in point 3 of section III of the Recommendation.

Therefore, in order to consider access to the worker's equipment lawful to corroborate the correct compliance with the "security measures" referred to in the query, it would be necessary to first identify this risk, and determine if there are no alternative measures less

intrusive to make this check, as can be seen from the aforementioned regulations and jurisprudence.

v

Regarding question E): "That any action be scrupulous with the possibility of finding a document of a private nature, even though personal topics are prohibited in the work tools, taking care and avoiding in this case, any opening and access in this content", the following considerations must be made.

The inquiry refers to the fact that City Council officials received data protection training and that the City Council's security protocol provides, among others, that "the entity's resources cannot be used for private purposes".

For the purposes of data protection regulations, it must be taken into account - as can be seen from section III of Recommendation 1/2013 - that even if the City Council has determined that workers cannot use the equipment, or of e-mail for personal or non-work reasons (in the case at hand, the City Council's protocol would determine that "the entity's resources cannot be used for private purposes"), the worker will not always be able to avoid , for example, the use by third parties of these emails, to send you messages of a personal nature.

In the same way, although the City Council's protocol, based on the information available, indicates the prohibition of having personal documentation on the equipment that the company provides to workers, it cannot be ruled out that access to the worker's equipment , which may be lawful in the terms indicated, involve access to the worker's own pe

From the perspective of the principles of data protection, the provision set out in the consultation is positively valued, in the sense that the City Council's action will have to be scrupulous in the event that private type documentation is found, "avoiding in this case any opening and access" of these contents.

Regarding this, remember that the principle of minimization (art. 5.1.c) RGPD) requires that the processed data must be adequate, relevant and limited to what is necessary in relation to the purposes of the treatment. In the case at hand, given the aforementioned purposes (provided in article 87 LOPDGDD, in connection with the labor regulations studied), which can enable access and monitoring of the equipment that the company makes available to workers, no the access to private information, in the terms of the consultation, seems to be provided or justified, in principle.

Therefore, as the consultation itself points out, and in line with what this Authority is doing in Recommendation 1/2013, given the purposes of access to the worker's equipment as can be seen from the information provided, it would be necessary articulate the intervention in the worker's team, so as to avoid access to this content of a private type or unrelated to the documentation of the Regional Office.

In this sense, answering question F, it is appropriate to limit access to people who are strictly necessary for the exercise of their functions, to make the intervention based on a copy or duplicate of the stored information, without altering the information recorded by the team, and documenting both the intervention and subsequent actions, describing in detail the actions taken and the results obtained.

According to Recommendation 1/2013, in this case access should be carried out by the person designated by the security manager, in the presence of the worker or, if this is not possible, of the staff representative and the person instructor or inspector.

In relation to this issue, the consultation states "That access would be made by the external - IT - Systems Administrator".

Although the intervention of an external technician is foreseen, access to the worker's equipment, and the processing of the information accessed, must be carried out following the instructions of the City Council. In this case in which access is carried out by an external third party unrelated to the person in charge, it would be up to the City Council to establish how this access to the equipment and the consequent treatment of the information should occur, through 'a contract or agreement for commissioning the treatment, in the terms provided for in article 28 RGPD, to which we refer.

This, without prejudice to the fact that, whether the access is carried out from the City Council's own services, or if it is articulated through an assignment contract so that a third party outside the City Council can access it (such as an external company), any processing of personal data is subject to the necessary compliance with the principle of confidentiality (art. 5.1.f) RGPD), which obliges any person who accesses the personal data that may be contained in the documentation, files, or e-mail, if applicable, of the team of the worker in question.

It is the responsibility of the City Council, in any case, to inform any of the persons appointed to intervene in the access to the worker's equipment, of their duties and obligations in matters of security, and in particular of this duty of secrecy .

In this sense, as recommended by Recommendation 1/2013, in this sense it may be advisable to make the people involved in these operations sign a commitment of confidentiality with respect to the data to which they may have access.

VI

Regarding question G): "If they understand that this action must be communicated to the affected person, in case they consider that access can be made, even though the consultation is made from the perspective that the affected person does not provide your consent.", the following must be said:

As can be seen from article 87.3 in fine LOPDGDD, and as it is made clear not only in the RGPD and the aforementioned jurisprudence (STEDH Barbulescu and STC 61/2021, among others), but also in Recommendation 1/ 2013, taking into account that the monitoring of the equipment that the employer makes available to the workers can be considered an intrusive measure, it is necessary to ensure that the workers, in this case, the worker who is on leave, are aware of it.

As recommended by Recommendation 1/2013 (section III), access to the worker's email accounts and, by extension, we could add, to the equipment that he uses for work reasons, must be carried out in agreement with the rules of use approved by the company, "which must warn about the control mechanisms for the use of technologies that may affect people's privacy, the consequences that can be derived from the control and the guarantees for workers, especially the right to be informed."

Having said that, regarding when the worker should be informed given the purpose pursued, we recall that, as set out in section III of Recommendation 1/2013, in the case of access to guarantee the continuity of the City Council's activity in his absence,

in this case due to illness, of the worker, the latter should be notified beforehand, and with sufficient time before the intervention. Only if this prior communication was not possible, could the worker be informed later, as soon as possible.

With regard to access in order to detect possible misuse of the equipment by the worker, it is considered that the intervention should also be made known to the affected worker in advance, unless the City Council considers that this may hinder appropriate investigations.

Finally, remember that, in application of the obligations of the person in charge in the matter of data protection (arts. 12, 13 and 14 RGPD), the City Council must provide information to workers in relation to the possibility of exercising their rights 'access, rectification or deletion of your data, among others (arts. 15 et seq. RGPD). This, regardless of the legal basis of the treatment (art. 6.1 RGPD).

In accordance with the considerations made in this report in relation to the query raised, the following are made,

Conclusions

Access to the local equipment of the official who is on leave, with the purpose of guaranteeing the continuity of the activity in the absence of the employee and with the purpose of verifying possible misuse of the equipment by the employee and protect the integrity of the information, it can be considered lawful if it is justified by the concurrent circumstances.

It is necessary to articulate the intervention in the worker's team, so as to avoid access to content of a private type or unrelated to the documentation of the Regional Office.

Access with the purpose of guaranteeing the continuity of the activity in the absence of the worker, must be communicated in advance to the intervention, unless it is not possible. Access for the purpose of determining misuse of the equipment must also be made known to the worker, unless it hinders the appropriate investigations. It must be done in the presence of the employee or, if this is not possible, of the staff representative.

Access must be limited to strictly necessary persons who must be bound by the duty of confidentiality. Access must be made from a copy or duplicate of the stored information, without altering the information contained in the equipment, and documenting both the intervention and the subsequent actions, describing in detail the actions taken and the results obtained. If an external technician intervenes, the processing of the information should be specified in a contract or processing commission agreement.

Barcelona, July 29, 2021