apdcat
Autoritat Catalana de Protecció de Dades

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

File identification

Resolution of sanctioning procedure no. PS 13/2021, referring to the Catalan Health Institute (Vall d'Hebron University Hospital)

Background

1. On 06/05/2020, the Catalan Data Protection Authority received a letter from a person for which he made single complaints (no. IP 129/2020 and 130/2020) - one in his own name and another on behalf of his minor daughter - against the Catalan Institute of Health (Vall d'Hebron University Hospital), on the grounds of an alleged breach of the regulations on personal data protection.

Specifically, the complainant (Mr. (...)) complained of alleged improper access to his medical history and that of his younger daughter (Mrs. (...)) by Hospital staff , center to which he claimed not to be linked; and in order to substantiate his complaint, he provided the following documentation:

a) Letter of 04/05/2020 through which the Hospital responded to the complainant's request of 17/04/2020 in relation to the traceability of access to his HC (henceforth, HC DENUN). In this letter, the Hospital informed him that *"there are accesses that we have not been able to verify that are linked to professional health visits. We have asked the professionals to justify, in writing, the reason why they accessed their medical history".* This letter was accompanied by a copy of the log of accesses to the HC DENUN, which lists 10 accesses as "unauthorized" carried out between 07/05/2018 and 03/11/2020, all they carried out from the Service of (...) and (...) of the Hospital.
b) Letter of 04/05/2020 through which the Hospital responded to the complainant's request of 17/04/2020 in relation to the traceability of access to the HC of his daughter (henceforth, HC MINOR). In this letter, the Hospital informed him that *"there are accesses that we have not been able to verify that are linked to professional health visits. We have asked the professionals to justify, in writing, the reason why they accessed the medical history of their minor daughter".* This letter was accompanied by a copy of the HC MINOR access register, which lists 18 accesses as "unauthorized" carried out between 05/16/2018 and 03/11/2020, all they carried out from the Service of (...) and (...) of the Hospital.

2. The Authority opened a preliminary information phase in accordance with the provisions of article 7 of Decree 278/1993, of November 9, on the sanctioning procedure applied to the areas of competence of the Generalitat, and article 55.2 of Law 39/2015, of October 1, of the common administrative procedure of public administrations (from now on, LPAC), to determine if the facts were likely to motivate the initiation of a sanctioning procedure.

3. In this information phase, on 23/06/2020 the ICS was required to provide the following information related to the events reported:

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

- Identified the users who would have made the accesses qualified as "non-authorities" in the access register corresponding to the HC DENUN and the HC MINOR (letters a/ ib/ of the 1st antecedent).
- Justify each of the controversial accesses.

4. On 02/07/2020, the ICS responded to the aforementioned request providing, as indicated in its letter, *"the justification of the accesses made to the medical history of the person making the complaint and of his minor daughter".* For this purpose, a copy of the e-mails that different professionals had sent to the Hospital managers justifying the access they had made to the HC DENUN and/or the HC MINOR was provided.

4.1. Answers linked to access to the MINOR HC:

- Email of 04/20/2020 through which Dra. (...) stated that *"today I entered the patient's clinical history to check my access to May 2019. I did not find any notes in the clinical course, discharge document or medical care that required my entry to your medical history in a justified way. I also don't remember consciously entering the patient's medical history. I have no personal or working relationship with her (...) the only reason I can find for this would be that I left the SAP* [Clinical History Management Program] *open on some computer and that someone entered with my user".*
- Email of 04/30/2020 through which Dr. (...) stated that, having reviewed the patient's clinical history, *"there was nothing that could justify admission to the HC (neither pre-operatives, nor surgical interventions nor any other type of activity related to our scope of action) (...) I am very careful with the entries I make and normally I usually write down the reason for entry or write in the HC the activity that has been carried out. I don't leave my keys to anyone. But it is true that in the operating room computer, many times it happens that things come up to do and the SAP remains open, at the expense of another person being able to start browsing the HCs with my number.*
  I will try to be more careful with this issue from now on."

4.2. Answers linked to access to the HC DENUN and the HC MINOR

- Email of 04/27/2020 through which Ms. (...) stated that the access *"was not done with bad intentions, only to reassure a colleague who does not have access to the SAP".*

- Email of 04/20/2020 through which Dra. (...) stated that *"today I entered the medical records of the persons cited in the attached documents, in order to verify my access on 08/13/2019. However, I have not found any notes in the clinical course or document that would justify my entry, and I am also not aware of having entered these clinical records. (…) I also don't have any type of work or personal relationship with the people in question, in fact I don't know these people, and the only explanation I can find for this unjustified access is having forgotten to close my SAP, and that a person with bad intentions these medical records have been entered without me*

authorization (…) I do not have any type of interest apart from the assistance of entering a clinical history (…)".

- Email of 20/04/2020 through which Dr. (...) expressed the following: *"Comment to him the perplexity that we have stayed both my resident (...) and myself when receiving this message. We have been reviewing and we do not know that neither Mr. (...) like Mrs. (...)*
they have not been visited or treated, nor (...) nor in the operating room nor in any cabinet by us; and that in addition to the staff, we know absolutely nothing about them, so we assume that someone from the surgical area during the morning hours has used our SAP abierto and carried out clinical history searches without permission (…)"
The same Dr. (...), in a subsequent email dated 04/22/2020, also addressed to the Hospital's managers, added that: *"tonight it occurred to me that the (...) I think (...) it is about the(...)of the (...), (...) of the area (...), which some time ago, he could not specify how much, due to his personal situation ((...)) 2 or 3 times spaced out in time and always coinciding that the (...) had gone to the CAP emergency room for (...), (...), etc, she asked me a lot distressed for her(...)to open the HC for her to be calmer. As he always told me that he was visiting the girl, I assumed that he had the right to be informed. At no time was there any bad intention (...). What does not suit me are the times that the HC has been consulted with my SAP user, which makes me think that someone has used it on more than one occasion without my consent (...)".*

- Email of 21/04/2020 through which Dr. (...) stated that *"I have been reviewing my latest activities and I do not know or have carried out any procedure with these persons mentioned. They have probably used my SAP to get into the medical history."*

5. In view of the information provided by the ICS, on 07/09/2020 and 11/30/2020 the ICS was again required to provide additional information, specifically:

- Identified, as it had been requested in office on 06/23/2020, the users who would have made the accesses qualified as "non-authorities" listed in the access register of the HC DENUN and the MINOR HC.
- Provide the risk assessment document prepared by the ICS for application to the Hospital.
- Report if the Hospital plans to block the user's session in SAP due to inactivity.
- Report if the Hospital instructs the professionals with access to the SAP to block the session on the computer when it is not being used. If so, it must be documented.

6. On 20/07/2020 and 20/01/2021, the ICS responded to the previous requirements, stating the following:

- That the implemented system *"incorporates an inactivity check during the open work session so that after 60 minutes of no activity, SAP closes the session".*
- That *"the professionals who have access to the SAP are instructed in accordance with the Instruction on the use of information and communication technologies in the Administration of the Generalitat of Catalonia, applicable to the Catalan Institute of Salut",* which contemplates the duty

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

of employees not to leave digital devices unattended once the identification and authentication process has been completed without previously blocking access.

- *That "there are some corporate policies of the center that have been established in this respect. In this case, in the document "use of Information Technology (ICT) resources and non-automated documentation" on page 2 it is said that staff must refrain from "leaving unattended workstation once the identification and authentication process has been passed without previously blocking its access'; and, on page 4: "You cannot allow third parties to view the patient's data or those of other people on the computer screen. When not in use, you must lock the computer, exit the screen and turn off the computer.*

- That *"the staff has the information on the Generalitat de Catalunya staff portal (ATRI), and documents and corporate policies of the center are also forwarded".*
- That *"the instruction on the use of information and communication technologies in the Administration of the Generalitat of Catalonia" has been in force since 2012; and that "the version of the center's corporate policies that is provided to workers is from 2017, last updated in 2018".*

Together with this information, the ICS provided the following documentation:

a) Copy of the log of accesses to the HC DENUN in which the following accesses are recorded carried out all of them from the Hospital's (...) Service:

a.1) 6 accesses made on 07/05/2018, 08/01/2018, 10/09/2018, 11/12/2018, 01/18/2019 and 02/27/2019 with the user belonging to Dr. (...) -with the professional category of doctor-.

a.2) 1 access carried out on 09/13/2018 with the user belonging to Mrs. (...) -with the professional category of nurse-.

a.3) 1 access carried out on 08/13/2019 with the user belonging to Dra. (...) -with the professional category of doctor-.

a.4) 1 access carried out on 20/11/2019 with the user belonging to Dra. (...) -with the professional category of doctor-.

a.5) 1 access carried out on 11/03/2020 with the user belonging to Dr. (...) -with the professional category of doctor-.

b) Copy of the register of accesses to the MINOR HC in which the following accesses taken are recorded carried out all of them from the Hospital's (...) Service.

b.1) 9 accesses made on 16/05/2018 (1), 05/07/2018 (1), 09/07/2018 (1), 01/08/2018 (1), 09/10/2018 (1),12/11/2018 (3 accesses that can be considered a single access as they are consecutive), 18/01/2019 (1), 27/02/2019 (1) and 11/06/2019 (1) , with the user belonging to Dr. (...) - with the professional category of doctor

b.2) 1 access (2 accesses that can be considered 1 as they are consecutive) carried out on 09/13/2018 with the user belonging to Ms. (...) -with the professional category of nurse-

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

b.3) 1 access carried out on 08/02/2019 with the user belonging to Dr. (...) -with category medical professional
b.4) 1 access carried out on 03/05/2019 with the user belonging to Dra. (...) -with professional category of doctor b.5) 1 access carried out on 08/13/2019 with the user belonging to Dra. (...) - with professional category of doctor b.6) 1 access carried out on 20/11/2019 with the user belonging to Dra. (...) -with

professional category of doctor of the Service of (...)-.
b.7) 1 access carried out on 03/11/2020 with the user belonging to Dr. (...) -with category medical professional

c) Extract from the Hospital's *"incident register"* in which there is an entry dated 05/06/2020 indicating that *"there are UNJUSTIFIED accesses"* to the HC DENUN and the HC MINOR, which *"* are *they have asked for allegations* [from the professionals who have accessed]" and that *"the file is handed over to legal medicine for reserve investigation".*

d) Copy of the following documents: *"Risk Assessment Report - SAP", "Workplace Risk Prevention Reception Manual", "Functions and obligations of users and employees. Use of Information Technology (ICT) resources and non-automated documentation";* and, *"Data Protection of Hospital Users".*

7. On 03/04/2021, the director of the Catalan Data Protection Authority agreed to initiate a sanctioning procedure against the ICS for an alleged infringement provided for in article 83.5.a), in relation to article 5.1.f); both of Regulation (EU) 2016/679 of the European Parliament and of the Council, of April 27, relating to the protection of natural persons with regard to the processing of personal data and the free movement thereof (hereinafter, RGPD). This initiation agreement was notified to the imputed entity on 09/03/2021.

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

9. On 15/03/2021, the ICS made objections to the initiation agreement.

10. On 28/04/2021, the instructor of this procedure formulated a resolution proposal, by which she proposed that the director of the Catalan Data Protection Authority admonish the ICS as responsible for an infringement provided for in article 83.5.a) in relation to article 5.1.f), both of the RGPD.

This resolution proposal was notified on 03/05/2021 and a period of 10 days was granted to formulate allegations.

11. The deadline has been exceeded and no objections have been submitted to the proposed resolution.

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

proven facts

By means of the user codes linked to different people who provide service at the Vall d'Hebron University Hospital (dependent on the ICS), the medical history of the complainant here (HC DENUN) and that of the his minor daughter (MINOR HC), without these accesses being related to any welfare action. The details of improper access to each of the clinical histories are as follows:

a) Access to the HC DENUN made all of them from the Service d(...) of the Hospital:

a.1) 6 accesses made on 07/05/2018, 08/01/2018, 10/09/2018, 11/12/2018, 01/18/2019 and 02/27/2019 with the user belonging to Dr. (...) -with the professional category of doctor-.

a.2) 1 access carried out on 09/13/2018 with the user belonging to Ms. (...) -with the professional category of nurse-.
a.3) 1 access carried out on 08/13/2019 with the user belonging to Dra. (...) -with the professional category of doctor-.
a.4) 1 access carried out on 20/11/2019 with the user belonging to Dra. (...) -with the professional category of doctor -.
a.5) 1 access carried out on 11/03/2020 with the user belonging to Dr. (...) -with the professional category of doctor-.

b) Access to the HC MINOR, also all of them carried out from the Service d(...) of the Hospital.

b.1) 9 accesses made on 16/05/2018 (1), 05/07/2018 (1), 09/07/2018 (1), 01/08/2018 (1), 09/10/2018 (1),12/11/2018 (3 accesses that can be considered a single access as they are consecutive), 18/01/2019 (1), 27/02/2019 (1) and 11/06/2019 (1) , with the user belonging to Dr. (...) - with the professional category of doctor
b.2) 1 access (2 accesses that can be considered 1 as they are consecutive) carried out on 09/13/2018 with the user belonging to Mrs. (...) - with professional category of nurse

b.3) 1 access carried out on 08/02/2019 with the user belonging to Dr. (...) -with category medical professional
b.4) 1 access carried out on 03/05/2019 with the user belonging to Dra. (...) -with professional category of doctor b.5) 1 access carried out on 08/13/2019 with the user belonging to Dra. (...) - with professional category of doctor b.6) 1 access carried out on 20/11/2019 with the user belonging to Dra. (...) -with

professional category of doctor of the Service of (...)-.
b.7) 1 access carried out on 03/11/2020 with the user belonging to Dr. (...) -with the professional category of doctor-

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

Fundamentals of law

1. The provisions of the LPAC, and article 15 of Decree 278/1993, according to the provisions of DT 2a of Law 32/2010, of October 1, of the Catalan Data Protection Authority. In accordance with articles 5 and 8 of Law 32/2010, the resolution of the sanctioning procedure corresponds to the director of the Catalan Data Protection Authority.

2. The accused entity has not made allegations in the resolution proposal, but it did so in the initiation agreement. Regarding this, it is considered appropriate to reiterate below the most relevant part of the motivated response of the instructing person to these allegations.

In its statement of objections to the initiation agreement, the ICS stated that the entity has implemented certain security measures and corporate policies in order to comply with data protection regulations; among them, the automatic closing of the SAP session due to inactivity; and, has given instructions to the professionals *"not to leave the workstation unattended once the identification and authentication process has been completed without first blocking its access".* That is why the imputed entity maintains that *"the ICS's fault does not exist",* and that *"it is not reasonable to impute to this institution the facts that some professionals have committed by using their login incorrectly"* and even less when *"this Every time the Institute detects that there has been improper access, it opens a reserved information procedure"* in order to resolve any disciplinary responsibilities that its staff may have incurred. In this sense, the ICS maintained that none of the workers listed in the access registers *"improperly entered"* the indicated clinical histories, since the accesses recorded there as having been made by users linked to these professionals, would have carried out by an unidentified person taking advantage of having left the SAP session open. And they added that, regarding the *"suspicion"* mentioned by one of the professionals *"toward a (...),(...) of the minor. This fact will be the subject of the corresponding reserved information"*

As the instructor highlighted in the resolution proposal, it must be clarified that in this procedure, the lack of security measures is not penalized, but the confidentiality of the data has been breached, and that this obligation to guarantee the confidentiality of the data is provided for in article 5.1.f) of the RGPD and 5 of Organic Law 3/2018, of December 5, on the Protection of Personal Data and guarantee of digital rights (hereinafter, LOPDGDD), and has a different content to the obligations described in articles 25 and 32 of the RGPD, linked to security measures. In other words, one thing is the obligation of the person responsible or in charge of the treatment to implement the relevant technical and organizational measures in order to avoid the loss, destruction or accidental damage of the data or their improper treatment authorized or illegal; and another is the duty of confidentiality incumbent on those in charge, in charge and all the people who provide service in their organizations in relation to the data subject to treatment. Therefore, there can be a violation of the confidentiality of the data, as is the case we are dealing with here, regardless of whether the person responsible or

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

in charge of the treatment have security measures implemented. And in the case analyzed here, the violation of confidentiality is considered proven since certain people from the organization (some of them identified, as will be seen later) accessed the HC DENUN and the HC MINOR, without their consent, and without this access being justified for any welfare reason.

With regard to the concurrence of guilt, this Authority agrees with the ICS that the commission of the imputed offense would be materially attributable to specific people who provide services in said institution. Having said that, it should be noted that, according to the system of responsibility provided for in the RGPD and particularly in article 70 of the LOPDGDD, responsibility for breaches of data protection regulations falls, among others, on those responsible of the treatments, and not about their staff. Specifically, the mentioned article 70 of the LOPDGDD establishes that:

"Responsible subjects.
1. They are subject to the sanctioning regime established by Regulation (EU) 2016/679 and this Organic Law:
a) Those responsible for the treatments.

So things are, in accordance with the responsibility regime provided for in the data protection regulations and from the point of view of the right to the protection of personal data, the person responsible for the facts that are considered proven is the ICS, given his status as responsible for the treatment in relation to which the offense alleged here has been committed.

Certainly, the principle of culpability, that is to say, the need for there to be intent or fault in the punitive action, is fully applicable to administrative sanctioning law, in accordance with what is provided for in article 28 of Law 40/2015, of October 1, of the legal regime of the public sector. This need for culpability as a constitutive element of the administrative offense has been expressly recognized by the Constitutional Court in its ruling 76/1990. However, it should also be noted that the Constitutional Court recognizes, in this same sentence, that the reception of the constitutional principles of the criminal order in the penal administrative law cannot be done mechanically and without nuances, that is, without weighing the aspects that differentiate one and another sector of the legal system. Therefore, starting from this premise, the question of the responsibility of legal entities will be analyzed next, specifically, their responsibility towards the acts of their employees.

The Supreme Court has established the responsibility of the legal person in these cases, taking into account the existence of a fault *"in eligendo"* or *"in vigilando".* Thus, in the STS of 28/11/1989, relating to a penalty imposed for violation of a Municipal Regulation in the matter of central markets, the Court argued the following:

"For this, the aforementioned article 68 of the Regulation establishes the direct administrative responsibility of the user or concessionaire for faults of this nature (contrary to the Regulation) committed by employees or family members in their service; precept that has its coverage in the municipal faculties to organize the operation of the public service of the market and to which

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

the penal principles that the appealed sentence improperly applies to proclaim its ineffectiveness are not applicable; residing the correct basis of the administrative responsibility of the employer for the faults of the employees or family members in his service and committed on the occasion of providing it, in the fault "in eligendo" or/ and in the "in vigilando", with millennial roots in the common law, as stated in the Judgment of the former 3rd Chamber of this High Court of April 29, 1988; in the same way that, and with the same foundation, the jurisprudence declares with a general character in the field of penal administrative law, the responsibility of legal persons for the actions of their dependents and employees."

With regard to the administrative responsibility of legal entities, it is of interest the Sentence of the Constitutional Court no. 276/1991, in which the highest interpreter of the Constitution pronounced in the following terms:

"In this respect, we must remember now that although it is true that this Constitutional Court has repeatedly declared that the principles inspiring the criminal order are applicable, with certain nuances, to the sanctioning administrative law, given that both are manifestations of the punitive order of the State - STC 18/1987 por todas-, it is not least that we have also alluded to the caution with which it is advisable to operate when it comes to transferring constitutional guarantees extracted from the criminal order to the sanctioning administrative law. This operation cannot be done automatically, because the application of these guarantees to the administrative procedure is only possible to the extent that they are compatible with their nature -STC 22/1990)-. Specifically, on guilt, this Court has declared that, in effect, the Spanish Constitution undoubtedly enshrines the principle of guilt as a basic structural principle of criminal law and has added that, however, the constitutional enshrining of this principle does not imply in any way that the Constitution has converted into a norm a certain way of understanding it -STC 150/1991-. This principle of culpability also governs matters of administrative infractions, because to the extent that the sanction of said infraction is one of the manifestations of the ius puniendi of the State, a regime of objective or no fault liability is inadmissible in our system - STC 76/ 1990-.

Even this Court has qualified as "correct" the principle of personal responsibility for own actions -principle of the personality of the penalty or sanction- (STC 219/1988). All this, however, does not prevent our Administrative Law from admitting the direct responsibility of legal persons, recognizing them, pues, infringing capacity. This does not mean, at all, that for the case of administrative offenses committed by legal persons the subjective element of guilt has been suppressed, but simply that this principle must necessarily be applied in a different way to how it is done with respect to persons physical

This different construction of the imputability of the authorship of the infringement to the legal person is born from the very nature of legal fiction to which these subjects respond. They lack the volitional element in the strict sense, but not the ability to infringe the rules to which they are subject.

So, with regard to the responsibility of legal entities in relation to the actions of their employees, it must be what has been decided by the Constitutional Court, which has been inclined

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

for the thesis of the existence of a fault *in eligendo* or *in vigilando* on the part of the legal person in these cases.

And collecting this doctrine of the Constitutional Court in relation to the culpability of legal entities, the Supreme Court pronounces itself in the following terms in the Judgment dated 04/15/1996:

"According to this latest jurisprudential doctrine, banking and credit institutions are administratively responsible for the negligence of their employees in the use of the security measures mandatorily installed in compliance with the current provisions, except when such action is not the result of inattention but of circumstances or situations of serious personal risk for the own employees or third parties. Neither the principle of typicality of the infraction nor that of the personality of the sanction are violated with such an interpretation because, in the scope of the sanctioning Administrative Law, legal persons can incur liability for the actions of their dependents, without being able to excuse themselves, as rule, in the behavior observed by them.

The art. 9 of Royal Decree Law 3/1979 refers to non-compliance with security regulations to companies, that is to say, to the owner of the same, not to their dependents or employees, which in the case of not attending to the instructions given by him on the compliance of the security rules could incur liability, but not in front of the Administration, but in front of its principal. The above-mentioned sentences express that the exposed doctrine does not suppose a preterition of the principles of culpability or imputability but its adaptation to the effectiveness of the legal obligation to comply with the security measures imposed on companies, a duty that entails, in case of non-compliance , the corresponding responsibility for the owner of the same, although it has its origin in the action of the employees to whom the employer had entrusted its effective implementation, direct responsibility that takes on greater meaning when the owner of the company is a legal person, constrained, by the demands of its own nature, to act through natural persons, a solution also advocated by the Constitutional Court Sentence 246/1991, of December 19, whose doctrine has been, to a large extent, determinant of the change in orientation of the jurisprudence of this Supreme Court, breaking with the thesis supported by the judgment appealed with foundation or in the previous jurisprudence that it cites, just as the procedural representation of the appealed banking entity does in its pleadings."

Judgment no. is also of interest in this regard. 339/2010, of 26/11/2010 (RCA no. 52/10, ordinary procedure) issued by the Administrative Court no. 1 of Barcelona, which confirms the sanctioning Resolution issued by this Authority on 26/11/2009, in which a Public Administration was declared responsible for the serious infringement provided for in article 44.3.g), in relation with article 10, both of the currently repealed Organic Law 15/1999, of December 13, on the protection of personal data, due to the fact that one of its employees had disclosed information about traffic violations contained in the system of management of fines.

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

"The person responsible for the file is the City Council, an organization that is required to maintain secrecy pursuant to art. 10 of the LOPD. This Administration imposes traffic sanctions, through its agents and bodies, collects the information to be able to process the files.
In the present case, therefore, the breach of the duty of secrecy on the part of the City Council is sanctioned, for not having guaranteed confidentiality in a matter processed by the City Council, allowing personal information to be passed on to third parties
not legitimized."

And finally, the sentence of the National Court of 02/22/2019 is also illustrative. In this case, the appellant entity - which had been sanctioned by the Spanish Data Protection Agency - based its appeal, among others, on the violation of the principle of culpability and argued in this regard that *"it was formed in the people who were going to make the visits and were provided with materials on how they should behave. At all times the objective was to comply with the LOPD, and the collection of any personal data was prohibited, unless the affected person so consented, and the only data that had to be collected were those contained in the Form. The AEPD, without motivating the concurrence of culpability, imputes the infringing conduct to the (…) and (…)."*

Well, the National Court considered that in this case there was culpable conduct on the part of the entity that had been sanctioned by the AEPD, *"conduct that constitutes an administrative offense - article 44.4.b) of the LOPD in relation to article 7 of the same- which requires the existence of guilt, and is specified, in the present case, in the collection of personal data relating to ideology with respect to persons who have denied their consent for said data treatment, or with respect to persons who they did not even know that said collection of personal data was taking place.*
Lack of diligence that constitutes the element of culpability of the administrative offense and is imputable to the appellant entity, and that does not require the concurrence of intent".

In accordance with all the above, it must be concluded that the responsibility of the ICS is linked to the performance of its employees; so that it is the culpable action of these, as a result of the violation of their obligations of reservation and confidentiality of personal data, which grounds the responsibility of the ICS in this sanctioning procedure for the acts materially committed by its staff

Finally, it is worth saying that the possible actions that the ICS can initiate against its employees – as material authors of the facts - in order to demand eventual disciplinary responsibilities, does not exempt the ICS, as responsible for the treatment, from its administrative responsibility in application of the sanctioning regime provided for in the data protection regulations. In relation to the eventual disciplinary actions that the ICS may carry out, it is worth saying that both article 77.3 of the LOPDGDD, and article 21.2 of Law 32/2010 provide that the Authority, apart from 'impose the sanction of reprimand (to the entities related to article 77.1 LOPDGDD) for the offense committed, it can also propose the initiation of disciplinary actions against the employee who has materially committed the offence. That is to say, that the possible disciplinary actions carried out by the data controller do not in any case replace the

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

responsibilities that are enforceable as such, by application of the RGPD and LOPDGDD sanctioning regime.

In accordance with what has been explained, this Authority considers that in the present case the culpability element required by the regulations and jurisprudential doctrine is present and that allows the ICS to be charged with the commission of the offense which is detailed below.

Therefore, the allegations made by the ICS in this procedure cannot be accepted.

3. In relation to the facts described in the proven facts section, relating to the principle of confidentiality, it is necessary to refer to article 5.1.f) of the RGPD, which provides for the following:

> *"1. The personal data will be:*
> *(…)*
> *f) processed in such a way as to guarantee an adequate security of personal data, including protection against unauthorized or illegal processing and against its loss, destruction or accidental damage, through the application of appropriate technical or organizational measures ("integrity and confidentiality»).*

On the other hand, the LOPDGDD, establishes the following in its article 5, relating to the duty of confidentiality:

> *"1. Those responsible and in charge of data processing as well as all the people who intervene in any phase thereof are subject to the duty of confidentiality referred to in article 5.1.f) of Regulation (EU) 2016/679.*
> *2. The general obligation indicated in the previous section is complementary to the duties of professional secrecy in accordance with its applicable regulations (...)"*

The health legislation, applicable to the case, regulates the use of the clinical history in the following terms:

- Article 11 Law 21/2000, of 29 December, on the rights of information concerning the patient's health and autonomy, and clinical documentation:

> *Uses of clinical history*
>
> *1. The clinical history is an instrument primarily intended to help guarantee adequate assistance to the patient. For this purpose, the care professionals of the center who are involved in the diagnosis or treatment of the patient must have access to the clinical history.*
>
> *2. Each center must establish the mechanism that makes it possible that, while assistance is provided to a specific patient, the professionals attending to him can, at all times, have access to the corresponding clinical history.*

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

3. The clinical history can be accessed for epidemiological, research or teaching purposes, subject to the provisions of Organic Law 15/1999, of December 13, on the protection of personal data, and the Law of State 14/1986, of April 25, general health, and the corresponding provisions. Access to the clinical history for these purposes obliges the preservation of the patient's personal identification data, separate from those of a clinical care nature, unless the latter has previously given consent.

4. The staff who take care of the administration and management tasks of the health centers can access only the data of the clinical history related to said functions.

5. The personnel in the service of the Health Administration who perform inspection functions, duly accredited, can access the clinical histories, in order to check the quality of the assistance, the fulfillment of the patient's rights or any other obligation of the center in relation to patients or the Health Administration.

6. All staff who use their powers to access any type of medical history data remain subject to the duty of confidentiality.

- Article 16 of Law 41/2002, of November 14, *"basic regulation of patient autonomy and rights and obligations in the field of clinical information and documentation"*:

"Article 16. Uses of clinical history.

1. The clinical history is an instrument primarily intended to guarantee adequate assistance to the patient. The healthcare professionals of the center who carry out the diagnosis or treatment of the patient have access to the patient's clinical history as a fundamental tool for their adequate assistance.

2. Each center will establish the methods that enable access to the clinical history of each patient at all times by the professionals who assist them.
3. Access to clinical history for judicial, epidemiological, public health, research or teaching purposes is governed by the provisions of current legislation on the protection of personal data, and Law 14/1986, of April 25, General of Health, and other rules of application in each case. Access to the clinical history for these purposes requires the preservation of the patient's personal identification data, separate from those of a clinical and healthcare nature, so that, as a general rule, anonymity is ensured, unless the patient himself has given his consent to don't separate them.

The investigation cases provided for in Section 2 of the Seventeenth Additional Provision of the Organic Law on the Protection of Personal Data and Guarantee of Digital Rights are excluded.

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

Likewise, cases of investigation by the judicial authority in which the unification of identifying data is considered essential are excluded
with the clinical care, in which it will be what the judges and courts have in the corresponding process. Access to the data and documents of the clinical history is strictly limited to the specific purposes of each
case

When it is necessary for the prevention of a serious risk or danger to the health of the population, the health administrations referred to in Law 33/2011, of October 4, General Public Health, will be able to access the identifying data of patients for epidemiological or public health protection reasons. Access must be carried out, in any case, by a healthcare professional subject to professional secrecy or by another person subject, likewise, to an equivalent obligation of secrecy, with prior motivation on the part of the Administration that requested access to the data.

4. The administration and management staff of the health centers can only access the clinical history data related to their own functions.
5. Duly accredited health personnel who carry out inspection, evaluation, accreditation and planning functions have access to clinical records in the fulfillment of their functions of checking the quality of care, respect for patient rights or any other obligation of the center in relation to patients and users or the health administration itself.

6. The personnel who access the clinical history data in the exercise of their functions are subject to the duty of secrecy.
7. The Autonomous Communities will regulate the procedure so that there is a record of access to the clinical history and its use".

During the processing of this procedure, the fact described in the proven facts section, which is considered constitutive of the violation provided for in article 83.5.a) of the RGPD, which typifies as such the violation of *"the basic principles for treatment",* among which the principle of confidentiality is at the top.

The conduct addressed here has been included as a very serious infraction in article 72.1.a) of the LOPDGDD, in the following form:

"The violation of the duty of confidentiality established by Article 5 of this Organic Law"

4. Article 77.2 LOPDGDD provides that, in the case of infractions committed by those in charge or in charge listed in art. 77.1 LOPDGDD, the competent data protection authority:

"(...) must issue a resolution that sanctions them with a warning. The resolution must also establish the measures to be adopted so that the conduct ceases or the effects of the offense committed are corrected.

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

The resolution must be notified to the person in charge or in charge of the treatment, to the body to which it depends hierarchically, if applicable, and to those affected who have the status of interested party, if applicable."

And section 3 of art. 77 LOPDGDD, establishes that:

"3. Without prejudice to what is established in the previous section, the data protection authority must also propose the initiation of disciplinary actions when there are sufficient indications to do so. In this case, the procedure and the sanctions that must be applied are those established by the legislation on the disciplinary or sanctioning regime that is applicable.
Also, when the infractions are attributable to authorities and managers, and the existence of technical reports or recommendations for the treatment that have not been properly attended to is proven, in the resolution in which the penalty is imposed, to include a warning with the name of the responsible position and it must be ordered to be published in the "Official Gazette of the State" or the corresponding regional newspaper.

In terms similar to the LOPDGDD, article 21.2 of Law 32/2010, determines the following:

"2. In the case of violations committed in relation to publicly owned files, the director of the Catalan Data Protection Authority must issue a resolution declaring the violation and establishing the measures to be taken to correct its effects . In addition, it can propose, where appropriate, the initiation of disciplinary actions in accordance with what is established by current legislation on the disciplinary regime for personnel in the service of public administrations. This resolution must be notified to the person responsible for the file or the treatment, to the person in charge of the treatment, if applicable, to the body to which they depend and to the affected persons, if any".

As explained by the instructor in the resolution proposal, in the present case, given the specific circumstances of the infringement that is declared here, relating to specific events already completed, this Authority does not consider it appropriate to propose the adoption of measures to correct the effects of the offense committed, without prejudice to what will be explained below.

Article 21.2 of Law 32/2010, in accordance with the provisions of article 77.3 of the LOPDGDD, foresees the possibility that the director of the Authority proposes the initiation of disciplinary actions, in accordance with what establishes the legislation in force on the disciplinary regime of personnel in the service of public administrations.

The facts that are imputed here and are qualified as constituting a very serious infringement for which the ICS must answer due to its status as responsible for the treatment, refer to actions that were materially carried out by employees of the ICS, and which could give rise to disciplinary actions.

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

In its statement of objections to the initiation agreement, the ICS asserted that none of the employees had improperly accessed the clinical records, and that the accesses contained in the records as carried out by the respective users were propitiated for having left themselves open to the SAP session, a circumstance that would have been taken advantage of by a third
person to access said stories. Well, this assertion, in accordance with the documentation provided by the ICS and contained in these actions, is not entirely accurate -
as evidenced by the instructor in the proposed resolution-, since Ms. (...) in the email he sent on 04/27/2020 to the Hospital's managers, he admitted to having accessed the said stories; and also Dr. (...) admitted to having accessed the MINOR HC, in the email of 04/22/2020 (section 4.2 of the 4th precedent), in both cases to do a favor to a colleague in care to their particular family circumstances.

In this regard, it should be noted that, although in similar cases of improper access to clinical records, the entity responsible for the treatment has been proposed to initiate disciplinary actions against the people who materially had unjustified access, in the case there are certain unique and exceptional circumstances that are recorded in the actions and that this Authority takes into account in order not to propose the initiation of disciplinary actions against these people.

At least, taking into account the high number of unauthorized access detected in the present case, this Authority requires the ICS to as soon as possible, and in any case within a maximum period of 15 days from the following day of the notification of the resolution, the unit responsible for human resources of the hospital addresses all the workers mentioned in the proven facts, reiterating to them their obligation as professionals not to access the clinical histories without a health care reason legitimi, as well as to close the SAP session in their absence; and expressly warning them that failure to comply with this obligation involves the commission of an infringement of the regulations on data protection that may lead to the initiation of disciplinary actions.

Once the corrective measure described has been adopted within the period indicated, within the next 10 days the ICS must inform the Authority.

For all this, I resolve:

1. Admonish the Catalan Institute of Health as responsible for an infringement provided for in the article 83.5.a) in relation to article 5.1.f), both of the RGPD.

2. Request the Catalan Institute of Health to adopt the corrective measure indicated in the 4th legal basis and accredit before this Authority the actions carried out by
fulfill them

3. Notify this resolution to the Catalan Health Institute.

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

4. Communicate the resolution to the Ombudsman, in accordance with the provisions of article 77.5 of the LOPDGDD.

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

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

If the imputed entity expresses to the Authority its intention to file an administrative contentious appeal against the final administrative decision, the decision will be provisionally suspended in the terms provided for in article 90.3 of the LPAC.

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

The director,