Autoritat Catalana de Protecció de Dades

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

File identification

Resolution of sanctioning procedure no. PS 49/2019, referring to the Enric Borràs Institute in Badalona, dependent on the Department of Education.

Background

1. On 02/10/2019 the Inspection Area of the Catalan Data Protection Authority became aware that, on 19/09/2019, the Business Insider media had published the following news regarding the Enric Borràs Institute of Badalona (hereinafter, the institute): *"A Catalan institute is using facial recognition to monitor class attendance, something for which a Swedish school has been fined 19,000 euros".*

2. The Authority opened a preliminary information phase (no. IP 262/2019), in accordance with the provisions of article 7 of Decree 278/1993, of November 9, on the sanctioning procedure of application to the areas of competence of the Generalitat, and article 55.2 of Law 39/2015, of October 1, on the common administrative procedure of public administrations (henceforth, LPAC), to determine whether the facts they were likely to motivate the initiation of a sanctioning procedure, the identification of the person or persons who could be responsible and the relevant circumstances involved.

3. In this information phase, on 08/10/2019, the Authority carried out an inspection at the institute's premises to verify certain aspects related to the facial recognition system of the students In that face-to-face inspection, the representatives of the institute and the Department of Education stated, among others, the following:

- That the facial recognition system had been installed since the 2011-2012 school year.
- That the purpose pursued was to reduce absenteeism, by monitoring student attendance, as well as informing families immediately in the event of absence.
- That the facial recognition system only applied to 1st year ESO students. In relation to students from other courses, attendance was checked manually by the teaching staff.

- That the system was suspended until the Authority made a decision. Attendance control via facial recognition had not been started this year. In the application that manages the attendance control, the data of several students started to be loaded (it was suspended before loading the entire list of students), but the vectors of their faces were not captured.

- That the system allowed the unique identification of people. The only identification problem that was detected involved two twin people, but that goes away

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

solve by verifying their identity through their fingerprint (the rest of the students did not have to identify themselves through their fingerprint).

- That at the beginning of the course, the student stood in front of one of the terminals, which collected the vectors of his face by making various movements. In turn, these vectors were associated with the student's code (it was a random code but unique for each student) and the phone number of the legal representatives.
- That to control their attendance, the student had to approach the terminal through which his identity was recognized.
- That when it was detected that a student had not attended the institute, before generating the warning (SMS), it was checked whether his family had warned that he would not attend. Otherwise, the person managing the attendance control application activated the option to send the SMS to their tutors. In the event that the family subsequently contacted the institute, indicating that the student had indeed attended, it was checked whether he had attended in person (the student was picked up in class).

ÿ That the 1st year ESO students, in addition to the attendance control through facial recognition, also had their attendance in class checked by passing a list.

- That the data needed to enable facial recognition were only kept during the 1st ESO course. In June, when the course ended, the data was deleted.
- That this treatment was based on the consent of the legal representatives of the students
- That in the event that the legal representative of a student does not grant consent or withdraws it later, the attendance of that student will be verified manually. No person had refused to give consent, nor had it been withdrawn.

ÿ That with regard to the rest of the high school students, whose presence was not controlled by facial recognition, the family was notified by phone if they did not attend the high school. The same would have been done in the event that the consent of the legal representatives of a 1st year student was not obtained. This warning was not immediate as in the case of the SMS that was sent regarding the students subject to facial recognition.

- That the right to information was made effective in the institute's educational commitment letter. In this letter, the possibility was not enabled that the legal representatives of minors could express their refusal to the processing of biometric data for the purposes of monitoring their children's attendance through facial recognition.

ÿ That the company installing the facial recognition system, carried out the maintenance of this system and intervened at the beginning of the course to load the students' data (associate the student's code with the name).

- That a data controller contract had not been signed with said company.
- That this system made it possible to achieve the goal of reducing school absenteeism.
- That another system to control attendance without facial recognition is being evaluated for next year.

- That there is a predisposition to act in accordance with the regulations on protection of data

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

Also, on this same date, the Authority's inspection staff verified, among others, the following:

- That in the lobby of the institute (ground floor) there were 2 terminals installed to allow the control of attendance through facial recognition. In turn, it was found that in the corridors of the 1st floor there were also 2 more terminals, one of which also allowed recognition by fingerprint.

- That the application that allowed the time control system to be managed was *"School Access Attendance Control",* which was installed on a computer located in the institute's secretariat. It will be verified that the system contained the data relating to the first and last names of several students, the group (class), the user ID and the mobile number of their tutor. It was found that the students were listed as absent and that they are all part of the 1st year of ESO. On the other hand, it will be verified that to access said application it was necessary to authenticate using a password.

Finally, the inspection staff collected the following documentation, which was delivered by the representatives of the inspected entity:

- Copy of the commitment letter signed by 2 legal representatives of 1st year ESO students (1 corresponding to the 2018-2019 academic year and the other 1 corresponding to 2019-2020).
- Copy of the image rights authorization form signed by 2 legal representatives (1 corresponding to the 2018-2019 academic year and the other 1 corresponding to 2019-2020).
- Copy of the technical specifications of access control using biometric systems for facial recognition and two budgets.

- Various documentation relating to facial recognition terminals.

4. On 29/11/2019, the director of the Catalan Data Protection Authority agreed to initiate a disciplinary procedure against the institute, firstly, for an alleged infringement provided for in article 83.5.a), in relation to articles 5.1.a) and 9; secondly, for an alleged violation provided for in article 83.5.b), in relation to article 13; and, thirdly, for an alleged violation provided for in article 83.4.a), in relation to article 28; all of them from Regulation (EU) 2016/679 of the European Parliament and of the Council, of 27/4, 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 12/12/2019.

5. On 20/12/2019, the institute made objections to the initiation agreement.

6. On 06/02/2020, the person instructing this procedure formulated a resolution proposal, by which he proposed that the director of the Catalan Data Protection Authority admonish the Enric Borràs Institute of Badalona as responsible, in the first place, for an infringement provided for in article 83.5.a) in relation to articles 5.1.a) and 9; secondly, of one

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

violation provided for in article 83.5.b) in relation to article 13; and thirdly, of an infringement provided for in article 83.4.a) in relation to article 28, all of them of the RGPD. This resolution proposal was notified on 06/02/2020 and a period of 10 days was granted to formulate allegations.

7. The deadline has been exceeded and no objections have been submitted.

proven facts

Of all the actions taken in this procedure, the facts detailed below are considered accredited.

1. The Enric Borràs high school in Badalona processed biometric data to control the attendance at the educational center of the 1st year of ESO students.

To this end, in the 2011-2012 academic year, he installed a facial recognition system to control attendance at the educational center of 1st year ESO students. And, in relation to two students who were twins, he also controlled their attendance by fingerprint, given that the facial recognition system did not guarantee their unique identification.

This attendance control system using facial recognition or fingerprint remained active until the end of the 2018-2019 school year. On 08/10/2019, the Authority's inspector staff verified that this system was no longer used to monitor the attendance of 1st grade students (who were listed as absent).

2. In relation to the control of the attendance of 1st year students by means of their facial recognition or fingerprints, the institute has not proven to have exercised the right of information to the representatives of 1st year students ESO during the 2018-2019 academic year.

3. In 2011, the institute commissioned the installation of said attendance control system for 1st year ESO students to the company Xip Solucions, SL; as well as its maintenance. The maintenance of this system meant that, at the beginning of each year, the staff of that company loaded the students' data into the system.

This assignment was not formalized in a contract or other written legal document with the content required by article 28.3 of the RGPD, and this was admitted by the person representing the institute in the face-to-face inspection carried out on 08/10/2019.

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 Authority

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

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.

2.1. About the news

In its statement of objections to the initiation agreement, the accused entity stated that the figures published in the media about the cost of installing the facial recognition system were not accurate; that the easy recognition system contributed to the improvement of absenteeism; that there was no *"intentional misuse of student data";* and that it had already been agreed to make a change of educational platform to manage attendance.

In advance, it should be made clear that the institute did not question in its statement of objections to the initiation agreement either the imputed facts, nor its legal qualification.

Having said that, with regard to the cost of implementation or maintenance, this was an irrelevant circumstance for the purposes of determining the imputed facts and their legal qualification.

In relation to the lack of intentionality invoked by the institute, as explained by the instructing person in the resolution proposal, it is necessary to point out that the types of offenders imputed in the present sanctioning procedure do not require the element of intentionality to be present .

Regarding the improvement of absenteeism, it is not discussed here whether the facial (and fingerprint) recognition system could contribute to achieving this goal, but that this could be obtained through other less intrusive means for the rights of 1st year ESO students, which did not involve the processing of special categories of data (such as biometric data).
Proof of the above is that with respect to the rest of the students, their attendance was controlled by the teaching staff at the institute or in the classroom; as well as the presence in the classroom of the 1st year of ESO students was also verified by the teachers passing a list (the controversial system verified the presence of students in high school, but not in the classroom).

It is worth saying that the Authority already pronounced itself in opinion CNS 63/2018, in the sense of considering that the *"principle of minimization is not manifested only when opting for alternatives that do not involve the processing of personal data , or to carry out the processing of data in such a way that the minimum indispensable data is used, but it must also mean that if a certain purpose can be achieved without having to process data of special categories, this*

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

option must prevail over other options that do involve the processing of these types of data."

Aside from the above, in the present case the treatment was not based on any of the exceptions established in article 9.2 of the RGPD, which must apply when special categories of data are treated, as was the case in the present case .

Finally, the decision on the change of educational platform to manage student attendance, would corroborate that in the present case it was not necessary to treat special categories of data to control student attendance who attended 1st year of ESO.

2.2. About the actions taken.

Subsequently, the accused entity informed in its statement of objections to the initiation agreement that the implementation of the system in this course was immediately suspended due to the news published in the media; that the terminals and the entire installation had been dismantled; as well as the secretarial IT team was also disabled.

In this sense, as stated by the instructing person in the resolution proposal, all the measures that the institute reported to have implemented following the face-to-face inspection carried out on 08/10/2019 by the Authority's inspector staff, must entail that it becomes unnecessary to require any corrective measures to correct the effects of the imputed violations, as will be explained later.

Likewise, it is necessary to emphasize the good predisposition of the institute to comply with the regulations on data protection, suspending the facial/fingerprint recognition system as soon as news was made public that questioned its adequacy to the data protection regime data; as well as when following the intervention of the Authority in the framework of the information phase, it has decided to dismantle said system.

On the other hand, in its statement of objections to the initiation agreement, the institute also indicated that no family *has "formally expressed any comment for the use of recognition".* At this point, it is sufficient to point out that this circumstance would not allow the processing of special categories of data to be considered lawful (Article 9 RGPD).

3. In relation to the facts described in point 1 of the proven facts section, both regarding facial recognition and fingerprint recognition, they violate the principles of legality (articles 5.1.ai 9 RGPD).

Article 5.1.a) of the RGPD regulates the principle of legality determining that the data will be *"treated in a lawful manner (...)".*

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

For its part, article 9.2 of the RGPD, regarding the treatment of special categories of data, provides that the prohibition of their treatment does not apply if one of the following circumstances is present:

> *"a) the interested party gives his explicit consent for the treatment of said personal data with one or more of the specified purposes, except when the Law of the Union or Member States establishes that the prohibition mentioned in section 1 cannot be lifted by the interested party;*
> *b) the treatment is necessary for the fulfillment of obligations and the exercise of specific rights of the person responsible for the treatment or of the interested party in the field of labor law and of social security and protection, to the extent that this is authorized by the Law of the Union of the Member States or a collective agreement in accordance with the Law of the Member States that establishes adequate guarantees of respect for the fundamental rights and interests of the interested party;*
> *c) the treatment is necessary to protect the vital interests of the interested party or another natural person, in the event that the interested party is not physically or legally able to give their consent;*
> *d) the treatment is carried out, within the scope of its legitimate activities and with due guarantees, by a foundation, an association or any other non-profit organization, whose purpose is political, philosophical, religious or trade union, provided that the treatment refers exclusively to current or former members of such organizations or persons who maintain regular contact with them in relation to their purposes and provided that personal data is not communicated outside of them without the consent of the interested parties;*
> *e) the treatment refers to personal data that the interested party has made manifestly public;*
> *f) the treatment is necessary for the formulation, exercise or defense of claims or when the courts act in the exercise of their judicial function;*
> *g) the treatment is necessary for reasons of an essential public interest, on the basis of the Law of the Union or of the Member States, which must be proportional to the objective pursued, essentially respect the right to data protection and establish measures adequate and specific to protect the fundamental interests and rights of the interested party;*
> *h) the treatment is necessary for the purposes of preventive or occupational medicine, evaluation of the worker's labor capacity, medical diagnosis, provision of health or social assistance or treatment, or management of health and social care systems and services, on the basis of the Law of the Union or of the Member States or by virtue of a contract with a healthcare professional and without prejudice to the conditions and guarantees contemplated in section 3;*
>
> *i) the treatment is necessary for reasons of public interest in the field of public health, such as protection against serious cross-border threats*

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

for health, or to guarantee high levels of quality and safety of health care and medicines or health products, on the basis of the Law of the Union or of the Member States that establishes measures
adequate and specific to protect the rights and freedoms of the interested party, in particular professional secrecy,
j) the treatment is necessary for archival purposes in the public interest, scientific or historical research purposes or statistical purposes, in accordance with article 89, paragraph 1, on the basis of the Law of the Union or of the Member States, which must be proportional to the objective pursued, essentially respect the right to data protection and establish appropriate and specific measures to protect the fundamental interests and rights of the interested party."

As indicated by the instructing person, during the processing of this procedure the conduct described in point 1 of the proven facts section (relating to facial recognition and fingerprint recognition) has been duly proven, which is constitutive of an infringement provided for in article 83.5.a) in relation to articles 5.1.a) and 9; both of the RGPD.

Article 83.5.a) of the RGPD, typifies as an infringement, the violation of the *"basic principles of the treatment, including the conditions for consent pursuant to articles 5, 6, 7 and 9",* among which contemplates the legality of the processing of special categories of data (articles 5.1.ai 9 RGPD).

For its part, this behavior has also been included as a very serious infringement in article 72.1.e) of Organic Law 3/2018, of December 5, on the Protection of Personal Data and guarantee of digital rights (in hereinafter, LOPDGDD), in the following form:

"e) The processing of personal data of the categories referred to in article 9 of Regulation (EU) 2016/679, without any of the circumstances provided for in the aforementioned precept and article 9 of this Law organic."

4. With regard to the fact described in point 2 of the proven facts section, regarding the violation of the right to information, it is necessary to refer to article 13 of the RGPD, which provides that:

"1. When personal data relating to an interested party is obtained, the data controller, at the time it is obtained, will provide all the information indicated below:

a) the identity and contact details of the person in charge and, where appropriate, of their representative;
b) the contact details of the data protection officer, if applicable;
c) the purposes of the treatment for which the personal data is intended and the legal basis of the treatment;

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

d) when the treatment is based on article 6, section 1, letter f), the legitimate interests of the person in charge or of a third party;
e) the recipients or the categories of recipients of the personal data, as the case may be;
f) in its case, the intention of the person in charge to transfer personal data to a third country or international organization and the existence or absence of an adequacy decision by the Commission, or, in the case of the transfers indicated in articles 46 or 47 or article 49, section 1, second paragraph, refers to the adequate or appropriate guarantees and the means to obtain a copy of these or the fact that they have been provided.
2. In addition to the information mentioned in section 1, the controller will provide the interested party, at the time the personal data is obtained, with the following information necessary to guarantee fair and transparent data processing:

a) the period during which personal data will be kept or, when not possible, the criteria used to determine this period;
b) the existence of the right to request from the person responsible for the treatment access to the personal data relating to the interested party, and its rectification or deletion, or the limitation of its treatment, or to oppose the treatment, as well as the right to the portability of the data ;
c) when the treatment is based on article 6, section 1, letter a), or article 9, section 2, letter a), the existence of the right to withdraw consent at any time, without it affecting the legality treatment based on consent prior to its withdrawal;

d) the right to present a claim before a control authority;
e) if the communication of personal data is a legal or contractual requirement, or a necessary requirement to sign a contract, and if the interested party is obliged to provide personal data and is informed of the possible consequences of not providing such data;
f) the existence of automated decisions, including the creation of profiles, referred to in article 22, sections 1 and 4, and, at least in such cases, significant information on the logic applied, as well as the importance and expected consequences of said treatment for the interested party. (...)"

In accordance with what has been presented, as indicated by the instructing person, the fact recorded in point 2 of the section on proven facts constitutes the infringement provided for in article 83.5.b) of the RGPD, which typifies as as such the violation of *"the rights of the interested parties pursuant to articles 12 to 22",* among which is the right of information of the interested person contemplated in article 13 of the RGPD.

In turn, this behavior has also been included as a very serious infraction in article 72.1.h) of the LOPDGDD, in the following form:

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

"h) The omission of the duty to inform the affected person about the processing of their personal data in accordance with the provisions of articles 13 and 14 of Regulation (EU) 016/679 and 12 of this Organic Law."

5. With regard to the fact described in point 3 of the proven facts section, regarding the lack of a data controller contract, it is necessary to refer to article 28.3 of the RGPD, which provides the following:

"3. The treatment by the controller will be governed by a contract or other legal act in accordance with the Law of the Union or the States, which binds the controller with respect to the controller and establishes the object, duration, nature and purpose of the treatment, the type of personal data and categories of interested parties, and the obligations and rights of the person in charge. Said contract or legal act will stipulate, in particular, that the manager:
a) will treat personal data solely following the documented instructions of the person in charge, including with respect to the transfer of personal data to a third country or an international organization, unless it is obliged to do so by virtue of the Law of the Union or of the Member States that applies to the person in charge; in such a case, the manager will inform the person in charge of that legal requirement prior to the treatment, unless such Law prohibits it for important reasons of public interest;
b) will guarantee that the persons authorized to treat personal data have committed to respect confidentiality or are subject to a confidentiality obligation of a statutory nature;
c) will take all the necessary measures in accordance with article 32;
d) will respect the conditions indicated in sections 2 and 4 to resort to another treatment manager;
e) will assist the person in charge, taking into account the nature of the treatment, through appropriate technical and organizational measures, whenever possible, so that he can comply with his obligation to respond to requests aimed at the exercise of the rights of the interested parties established in chapter III;

f) will help the manager to ensure compliance with the obligations established in articles 32 to 36, taking into account the nature of the treatment and the information available to the manager;
g) at the choice of the person responsible, will delete or return all personal data once the provision of the treatment services is finished, and will delete the existing copies unless the conservation of personal data is required under Union Law or member states;
h) will make available to the person in charge all the information necessary to demonstrate compliance with the obligations established in this article, as well as to allow and contribute to the performance of audits,

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

> *including inspections, by the person in charge or by another auditor authorized by said person in charge.*
> *In relation to what is provided in letter h) of the first paragraph, the person in charge will immediately inform the person in charge if, in his opinion, an instruction infringes the present Regulation or other provisions in the area of data protection of the Union or the Member States. "*

In accordance with what has been presented, as indicated by the instructing person, the fact recorded in point 3 of the section on proven facts constitutes the violation provided for in article 83.4.a) of the RGPD, which typifies as to such, the violation of *"the obligations of the person in charge and of the person in charge pursuant to articles 8, 11, 25 to 39, 42 and 43",* among which there is that provided for in article 28 RGPD.

In turn, this behavior has also been included as a serious infringement in article 73.k) of the LOPDGDD, in the following form:

> *"k) Entrust the processing of data to a third party without the prior formalization of a contract or other written legal act with the content required by article 28.3 of Regulation (EU) 2016/679."*

6. 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.*
> *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."*

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".*

In the present case, as explained by the instructing person in the resolution proposal, no requirement for corrective measures should be proposed to correct the effects of the

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

imputed infringements, given that the institute has dismantled the facial and fingerprint recognition system.

resolution

For all this, I resolve:

1. Admonish the Enric Borràs Institute of Badalona as responsible for three infringements: an infringement provided for in article 83.5.a) in relation to articles 5.1.a) and 9; another offense provided for in article 83.5.b) in relation to article 13; and a third violation provided for in article 83.4.a) in relation to article 28, all of them of the RGPD.

It is not necessary to require corrective measures to correct the effects of the infringement, in accordance with what has been set out in the 6th legal basis.

2. Notify the institute of this resolution.

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

4. 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,