File identification

Resolution of sanctioning procedure no. PS 41/2022, referring to the Foundation for the Open University of Catalonia

Background

1. On 04/11/2021, the Catalan Data Protection Authority received a letter from a person filing a complaint against the Foundation for the Open University of Catalonia (hereinafter, FUOC) on the grounds of an alleged breach of data protection regulations.

In particular, the complainant stated that the FUOC would be using a facial recognition tool in order to check the identity of the students during remote assessment tests. In this regard, he explained that the operation of this system requires, first of all, that the student captures an image of his face, so that the tool can compare it with his ID photograph, and verify that it is the person who claims to be Likewise, the photograph was also used to compare it with the images that are captured while the student takes the distance assessment test, for the purposes of verifying the student's identity. Then, the person making the complaint explained that it is mandatory to register with the facial recognition tool in order to be able to perform the evaluation tests.

In order to substantiate the facts reported, he provided various information, among which stands out an email that the FUOC would have sent him on 04/11/2021, the subject of which referred to "Virtual tests: haz *the register in the facial recognition tool* . By means of the aforementioned email, the complainant was informed that he could proceed to register in the facial recognition tool, in order to be able to validate his identity *"while doing the tests* ". Likewise, he was informed that " *the application will capture a series of photographs and compare them with the photograph of the identity document that you previously sent us to ensure that it was you." These images will be compared with the ones we capture while you do the final tests. For this reason, this step is essential to be able to make the final tests* ".

This complaint was assigned no. IP 448/2021.

2 . On the dates 16/11/2021, 01/12/2021, 27/04/2021 and 02/05/2022, four other people presented, respectively, four letters in which they denounced these same facts related to the use by the FUOC of the facial recognition tool in the evaluation tests.

These complaints were assigned the following numbers: IP 469/2021, IP 489/2021, IP 150/2022 and IP 158/2022, respectively.

3. The Authority opened a preliminary information phase, in accordance with what is provided for in 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, on the common administrative procedure of public administrations (from now on, LPAC), to determine if the facts were likely to motivate the initiation of a procedure punisher

4. In this information phase, on 03/05/2022 the Authority required the reported entity to report, among other issues, on the legal basis that would legitimize the use of a facial recognition system to evaluate the students, to argue the circumstance that would enable the

processing of special categories of personal data, to point out whether the students were offered the possibility of taking the tests remotely by means of another alternative system to facial recognition, and to indicate what the consequences would be for students who decide not to register for the facial recognition tool.

5. On 16/05/2022, the FUOC responded to the above-mentioned request in writing in which it set out the following:

- " *The legal bases that legitimize the implementation of this processing of personal data are two. On the one hand, the execution of the contract (verifying the identity of the person who performs the final evaluation test - hereinafter, "PAF") and, on the other, the legitimate interest in preventing and detecting fraud academic The treatment consisting in the verification of the identity of the people taking the PAF is an essential part of the contract for the provision of academic services, formalized between the student and our university, that is, the registration. Therefore, the legal basis that legitimizes the verification of the presence of the parties to the contract (registration) at the essential moment of the contractual relationship, as is the verification of knowledge (final test), is the execution of the contract.*
- The treatment consisting in the prevention and detection of fraud is based on the legitimate interest, in accordance with what is established in the same guidelines 2/2019 of the CEPD. The UOC carried out the corresponding weighting of the legitimate interest and has the evidence of this weighting.
- The UOC has not applied the legal basis of consent in this processing of personal data since, according to the doctrine of the CEPD and of APDcat itself , there is a risk that consent is not considered freely given in this case.
- The courses taught by the University are taught online (not face-to-face) and the assessment is generally carried out online, using identity verification tools in cases of assessment through PAF. This information reaches the student before the pre -contractual sentence, at the time when he collects the information about the training program he wants to take and, therefore, when he makes the decision to do it, he already knows the system of verification, both of knowledge and identity, that will be used by the University (...). Therefore, the student is aware and free when choosing a University and studies that suit their needs".

The FUOC also pointed out that the evaluation system of the students' learning process for each subject is established every semester in the corresponding teaching plan, and argued that the number of subjects that are evaluated through PAF is limited and that, for therefore, they will require identity verification. Likewise, it explained that the lack of identification of the person who presents himself to an online PAF in the framework of the contract for the provision of academic services means that the final qualification of "Not presented" is recorded in his academic file. And then he added:

- *Pursuant to what is established in the UOC Rights and Duties Regulations, which are published on the University's Electronic Site, the University also contemplates cases in which students with special needs, or with personal circumstances which, duly accredited, would justify a curricular adaptation and the possibility of being able to carry out a PAF without verification of their identity (...). The assumptions that enable the realization of the adapted PAF are those contemplated in the document attached as Annex 3.*

- *The University's internal regulations also provide for the possibility for the student to justify the need to take the test without using the facial recognition tool to verify their identity. In such a case, the verification of the student's identity is done manually.*
- *The first online PAF in which the facial recognition system was used to conduct online tests took place on January 8, 2022 (...).*
- *Out of a total of 75,024 students enrolled in the first semester of the 2021-2022 academic year, only 31,501 students have completed PAF with identity authentication.*

The reported entity attached various documentation to the letter. Among this information, he provided the Rights and Duties Regulations of the FUOC, which provides that the following people are exempt from the verification of identity through photographs: "a) *blind or severely visually impaired people b) people with mental disorders c) people with serious mobility problems".*

6. On 06/14/2022, the director of the Catalan Data Protection Authority agreed to initiate a sanctioning procedure against the FUOC for an alleged infringement provided for in article 83.5 a) in relation to article 5.1 a); all of them from 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 06/16/2022.

7. On 06/17/2022, the FUOC submitted a request to extend the period granted for the submission of objections to the initiation agreement indicated in the previous precedent.

8. On 06/28/2022, the instructor of the procedure agreed to extend the deadline requested by the FUOC, under article 32 of the LPAC.

9. On 07/08/2022, the accused entity made allegations to the initiation agreement, and provided various documentation with its letter.

10. On 10/13/2022, the FUOC submitted a letter expanding the allegations made on 07/08/2022, providing the documentation listed below, which would have been adapted as a result of the implementation of the facial recognition system in the performance of the final assessment tests, and this " *for the purposes of demonstrating that the FUOC acts with due diligence, as a guarantor of the academic rights of its students* ":

- *"Text of the current registration form.*
- *Text of the current General Conditions of Contract.*
- *Text of the current UOC Academic Regulations.*
- *Text of the current UOC Privacy Policy.*
- *Outline of the main communication actions aimed at students in relation to the final assessment tests and the use of facial recognition systems, and some examples of said communications".*

11. On 04/11/2022, the instructor of this procedure formulated a resolution proposal, by which she proposed that the director of the Catalan Data Protection Authority impose on the FUOC a fine of 20,000 euros (twenty -one thousand euros) as responsible for an

infringement provided for in article 83.5.a) in relation to articles 5.1.a) and 9; all of them from the RGPD.

This resolution proposal was notified on 04/11/2022 and a period of 10 days was granted to formulate allegations.

12. On 10/11/2022 the FUOC submitted a request to extend the deadline granted for the submission of allegations to the proposed resolution.

13. On 11/11/2022, the instructor of the procedure agreed to extend the deadline requested by the FUOC.

14. On 11/25/2022, the accused entity submitted a statement of objections to the proposed resolution, which are addressed in the 2nd and 5th legal bases of this resolution.

proven facts

From 08/01/2022, the date on which the Foundation for the Open University of Catalonia first used the facial recognition system to carry out online tests, and until 16/05/2022, there have been examined a total of 31,501 students using the aforementioned tool for the purposes of validating their identity while they took the distance assessment tests. In this regard, it should be noted that the FUOC warned students that registration in the facial recognition tool was essential in order to be able to take the assessment test and that, if they did not register, the final grade would be obtained of " *Not presented".*

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 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 formulated allegations in the resolution proposal, in which, in essence, it reiterates those it formulated in the initiation agreement, and which are analyzed below.

2.1. On the nature of biometric data and on the legitimate bases of the treatment.

In essence, the FUOC focuses on the first point of its allegations in arguing that, on the one hand, the biometric data it uses to verify the identity of the students, in the framework of the final assessment tests, are not special categories of data, and on the other hand, that the legal bases that legitimize the use of biometric data are the execution of a contract – university enrollment – and legitimate interest.

2.1.1. On the special category character of the biometric data used to verify the identity of the students in the framework of the assessment tests.

For the purposes of analyzing and interpreting article 9 RGPD, in relation to article 4.1.14 RGPD, the content of these precepts is reproduced below.

Article 4 *Definitions*

1.14) "biometric data": personal data obtained from a specific technical treatment, relating to the physical, physiological or behavioral characteristics of a natural person that allow or confirm the unique identification of said person, such as facial images or fingerprint data;

Article 9 *Treatment of special categories of personal data*

1. The processing of personal data that reveal ethnic or racial origin, political opinions, religious or philosophical convictions, or trade union affiliation, and the processing of genetic data, biometric data aimed at uniquely identifying a person are prohibited physical, data relating to health or data relating to the sex life or sexual orientation of a natural person.

2. Section 1 will not apply when one of the following circumstances occurs:
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 of the 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 to health, or to guarantee high levels of quality and safety of health care and medicines or sanitary products, on the basis of the Law of the Union or of the Member States that establishes appropriate and specific measures 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 proportionate 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.
3. The personal data referred to in section 1 may be processed for the purposes mentioned in section 2, letter h), when its treatment is carried out by a professional subject to the obligation of professional secrecy, or under his responsibility, in agreement with the Law of the Union or of the Member States or with the rules established by the competent national organisms, or by any other person also subject to the obligation of secrecy in accordance with the Law of the Union or of the Member States or of the rules established by the competent national bodies.
4. Member States may maintain or introduce additional conditions, including limitations, with respect to the treatment of genetic data, biometric data or health-related data.

As has been advanced, in its letter of objections to the proposal, the imputed entity reiterates the argument contained in the allegations in the agreement to initiate this procedure, defending the existence of two types of biometric data. On the one hand, those that aim to uniquely identify a person and, on the other hand, those that do not have the consideration of particularly protected data – such as the voice or a photograph – that aim to authenticate the identity of an individual. In this regard, the FUOC maintains that the processing of personal data by means of facial recognition, insofar as it verifies the student's identity, and does not aim to uniquely identify him, does not constitute processing of special categories of data . In this line, the accused entity defends that the differentiation between the two types of biometric data is based on criteria adjusted to Law and shared by the European Data Protection Committee, by Opinion 3/2012 issued by the Working Group of the article 29, and by Report 0036/2020 of the Spanish Personal Data Protection Agency (hereinafter, AEPD), among others.

In relation to the above, in the proposed resolution it was argued that Opinion 3/2012 issued by the Article 29 Working Group predates the entry into force of the RGPD and, therefore, it is carried out in a context in which the concept of biometric data does not fall within the consideration of a special category of data, a fact that, at present, would not be admissible in any case, in light of the definition of biometric data, provided for in article 4.14 RGPD. And, in this regard, the FUOC, in its statement of objections to the proposed resolution, defends the following:

"The fact that this date of 2012 (actually, before the entry into force of the RGPD) does not invalidate or contradict his considerations. Proof of this is that this Opinion was taken into consideration by the Spanish Data Protection Agency in its Report 0036/2020.

Likewise, there are pronouncements subsequent to the entry into force of the RGPD that support the same interpretation.
We pay special attention to these:

- *Organic Law 7/2021, of May 26, on the protection of personal data processed for the purposes of prevention, detection, investigation and prosecution of criminal offenses and the execution of criminal sanctions. The special category of the data is clearly identified if it is aimed at unique identification .*
  Preamble : Section IV (…) Biometric data (such as fingerprints or facial images) are only considered included in this special category when their treatment is aimed at uniquely identifying a natural person. (…)
  Article 13. Treatment of special categories of personal data. (…)
- *Guidelines 3/2019 on the processing of personal data through video devices, of the CEPD. Version 2.0 Adopted on January 29, 2020: the difference between whether the data has been technically treated in a specific way to contribute to the unequivocal identification of a person is particularly addressed (…)*
- *Guidelines 2/2021 on CEPD virtual voice assistants, version 2.0 Adopted on July 7, 2021. (…)"*

For all the above, the criterion consisting of distinguishing identification from authentication, mentioned in Opinion 3/2012, remains fully valid, regardless of the entry into force of the RGPD, there being a legislative will to do this distinction"

In relation to the above, the FUOC argues that, maintaining that its interpretation is not valid, generates legal defenselessness as a result of the discrepancy or lack of unitary criteria between different control authorities and that "it would require the necessary actions for *unification of criteria and obtaining a unique and coherent pronouncement".*

Regarding this, it is necessary to reiterate here what the instructor argued in the resolution proposal, highlighting that, pursuant to article 9.1 of the RGPD, the processing of biometric data aimed at identifying or authenticating is prohibited a person, unless one of the exceptions provided for in section 2 of the same precept applies. It is also necessary to cite Recital 51 of the RGPD, which specifies that " *(...) the treatment of photographs should not be systematically considered treatment of special categories of personal data, because they are only included in the definition of biometric data when the to be treated with specific technical means allow the univocal identification or authentication of a natural person. (...)"*

This Authority cannot share the interpretation of the imputed entity, which maintains that the verification or authentication of a person by means of facial recognition does not constitute a special category biometric data, in the terms established by article 9 RGPD. The criterion of this Authority, embodied in its Opinion CNS 21/2020, is clear when it maintains that article 9 of the RGPD, when it refers to the univocal identification of a person, includes the concepts of "authentication or verification", since both authentication and verification enable the unique identification of a person. In literal terms, the said Opinion argues the following:

"(...) it would not seem appropriate to exclude part of the biometric data (those that undergo a specific technical treatment in order to verify the identity of a person) from the enhanced protection that the RGPD recognizes for that data personal data that, due to their nature and the context in which they are processed, become particularly sensitive, in

view of the consequences that, for the people affected, may derive from their treatment, which would take place if they were not recognized as to special category of data.
It cannot be overlooked that identification and authentication, despite responding to different objectives, are closely linked concepts.
Identification aims to determine the identity (recognize) of a person (who are you?) based, in this case, on their physical, physiological or behavioral characteristics. The purpose of authentication is to use this data to confirm or deny the identity of this person (are you who you say you are?) and this action would imply, in any case, having previously identified this person.
When authentication is carried out, for example when a person is identified by fingerprint when entering work, in some cases it leads to a one-to-one identification (for example, if a marking card or a code to identify oneself) or it can operate as a one-to-many correspondence system (for example if the fingerprint of the worker who accesses the workplace is compared with that of all the workers in the company to finally determine who is the worker who has accessed).
It should be interpreted that when the GDPR refers to the unique identification of a natural person in Article 9.1, it is also referring to the authentication of that person's identity ("confirm").

Regarding the fact that other authorities - such as the Spanish Data Protection Agency - have defended the existence of two types of biometric data, it does not condition the criterion of this Authority, nor the meaning of this resolution, in the insofar as it is not subject to the interpretative criteria of other control authorities, with respect to which there is no subordination relationship.

In relation to the above, the FUOC argues that the lack *of "unitary criteria between different Control Authorities"* generates helplessness, and has pointed out that the necessary actions should be carried out for the unification of criteria.

However, in this regard, the accused entity cannot ignore the fact that Report 0036/2021 of the AEPD, invoked in its statement of objections and which, as it says, includes the criteria of the Group of the article 29, despite maintaining the existence of two categories of biometric data, it is clear when he concludes that, in the facial recognition processes used to carry out online assessments , the processing of biometric data is carried out with the purpose of uniquely identifying a person and constitutes, therefore, a treatment that falls within the prohibitions of article 9.1 RGPD.

2.1.2. On the legal bases that legitimize the treatment of controversial biometric data.

In its statement of objections to the proposal, the accused entity reproduces the legal arguments contained in the various documents presented to the Authority, as part of the present procedure, and reiterates that, the bases that legitimize the treatment are the execution of a contract - for the purpose and effect of *"verifying the identity of the person who takes the final assessment test - hereinafter, "PAF" -"* and the legitimate interest - to *"prevent academic fraud "-,* provided for, respectively, in article 6.1 sections b) and f) of the RGPD.

In accordance with the principle of legality, enshrined in article 5.1 a) of the RGPD, personal data must be treated *"in a lawful, fair and transparent manner in relation to the interested party ".* Therefore, in order for the processing of special category data - as is the case - to be

lawful, one of the legal bases of Article 6.1 of the RGPD must be met, which enable the processing of personal data, as well as any of the exceptions provided for in article 9.2 of the RGPD, which allow the general prohibition of article 9.1 of the RGPD to be lifted.

First of all, it must be shown that the accused entity starts from the premise that the biometric data in question does not have the condition of a special category of data, which is why it has not invoked in its pleadings any of the exceptions provided for in article 9.2 RGPD. In any case, it is not observed that any of the exceptions contained in the said article may apply. However, it is not superfluous to reproduce here the analysis carried out in the proposal on the two exceptions that, based on the legal bases of the treatment invoked by the FUOC, could have a certain relationship, such as the explicit consent given by the affected person , and the concurrence of an essential public interest (article 9.2 letters a/ ig/ RGPD, respectively).

With regard to consent, the FUOC itself recognized - and expressed this expressly in the framework of the previous information that preceded this procedure -, not having based the controversial treatment on consent, given that this could not be free, and thereby breaching one of the requirements that, among others, consent must meet in order to be considered validly given (art. 4.11, in connection with recitals 32 and 42 RGPD).

This Authority shares the criterion of the imputed entity that prevents students from being considered to be able to freely consent to the controversial data processing whenever, if they do not agree to submit to the facial recognition tool, they obtain the qualification of "Not submitted" and, therefore, they have no other alternative to take the final assessment tests (with the exception of some very specific exceptions – antecedent 5è in fine). And to the above it should be added that the consent given in the case in question here might not meet other conditions provided for by the regulations, such as that it be explicit.

Likewise, on the presumed existence of an essential public interest - art. 9.1.g) RGPD -, and in line with Opinion 17/2020 of this Authority, it should be noted that, when Recital 41 of the RGPD specifies that when the Regulation refers to a legal basis, it does not necessarily require that this it is a legislative act adopted by a Parliament, but it establishes that it will have to meet the requirements that the constitutional order of the Member State contemplates. And, in this respect, it must be made clear that, in accordance with the Spanish legal system, the rule that establishes the processing of personal data must have the status of law, in compliance with Article 53 CE, insofar as entails the limitation of a fundamental right, as recognized by the constitutional jurisprudence included in Opinion 17/2020 of this Authority (SSTC 292/2000, SSTC 76/2019, STJUE 08.04.2014, Digital Rights Ireland , among others).

In accordance with the above, given that there is currently no legal standard that enables universities and other teaching centers to process biometric data for this purpose (online assessments) , and given that none of the other exceptions in Article 9.2 RGPD apply, which could lift the prohibition in Article 9.1 RGPD, the existence of a legal basis that legitimizes the reported data processing must be ruled out.

Given the above, it would be unnecessary to address the legal bases invoked by the entity provided for in article 6 of the RGPD. Despite this, a brief analysis is made below.

Article 6.1 RGPD establishes that the treatment will be lawful if at least one of the following conditions is met:

"a) the interested party gives his consent for the treatment of his personal data for one or several specific purposes;
b) the treatment is necessary for the execution of a contract in which the interested party is a party or for the application at the request of this pre-contractual measures;
c) the treatment is necessary for the fulfillment of a legal obligation applicable to the person responsible for the treatment
d) the treatment is necessary to protect the vital interests of the interested party or another natural person;
e) the treatment is necessary for the fulfillment of a mission carried out in the public interest or in the exercise of public powers conferred on the person responsible for the treatment;
f) the treatment is necessary for the satisfaction of legitimate interests pursued by the person responsible for the treatment or by a third party, provided that these interests do not prevail over the interests or fundamental rights and freedoms of the interested party that require the protection of personal data, in particular when the interested party is a child. The provisions in letter f) of the first paragraph shall not apply to the processing carried out by public authorities in the exercise of their functions"

As has been advanced, the FUOC considers that the facial recognition system is necessary for the execution of the contract for the provision of non-face-to-face higher education services, signed between the imputed University and the student, in accordance with the article 6.1 b) RGPD, and argues:

" *The UOC provides a public education service that focuses on the realization of quality non-face-to-face studies. The training methodology of the UOC is based 100% on the online channel, so that online assessment becomes an essential part of the relationship between the student and the University (...).*
The justification of the contract is the formalization of the registration by the student in order to be able to take the corresponding studies. Therefore, its essence lies in enabling the provision of non-face-to-face higher education academic services required by the student, with the advantages and differential features offered by a non-face-to-face University such as the UOC (...).

The enrollment contract has the following essential elements:
I. The desire of the student to obtain non-face-to-face training services having chosen to train informed by a specific educational methodology on the rest of the training offer on the market
II. The free, voluntary and informed consent given by the student when signing the contract through the formalization of the corresponding registration; and,
III. The object of the contract to be signed, the provision of non-face-to-face higher education academic services, in accordance with an own didactic methodology aimed at responding to the educational needs of people who are trained throughout life, as indicated to the General Contract Conditions accepted by the student (...)

The student, when enrolling at the UOC, expects to receive a quality educational service with the advantages and flexibility of a non-face-to-face University and with all the guarantees of teaching quality required by university education, while preventing, detecting and combating irregular behavior resulting from an education in this modality, such as, among others, copying, plagiarism or impersonation (...) The student has the right to be assessed on his knowledge and skills in a fair and objective manner, in accordance with the principles of neutrality, objectivity, non-discrimination and equal opportunities, so that if the UOC did not do everything possible to avoid academic fraud in the knowledge verification processes and , would allow some students to pass final assessment tests using illicit or fraudulent means, would be frustrating the academic expectations of students who make the effort to study and expect others to behave in the same way, and could incur a breach of contract."

Likewise, the FUOC also maintains that the students who decide to study at this University are aware that the education provided by the University is in a virtual teaching mode, and not face-to-face, "while using identity verification *tools in the cases of assessment through final assessment tests".* And he adds that, before formalizing the contract with the future student, information is provided regarding the conditions for the provision of the academic service of a teaching nature, among which is included the one relating to the verification of both knowledge and identity, and that, therefore, the student " *(...) has the option of rejecting this data processing - necessary for the execution of the contract with the FUOC -, by enrolling in another educational center" .*

In accordance with the above, the imputed entity concludes that the student's identification data constitute an essential part of the enrollment and evaluation process, in order to ensure that the individual being examined is the same person than the one who enrolled for those specific studies. And about the student's consent, he adds that " *it must be understood that the signing of a contract, with the characteristics of the UOC enrollment process, implies an express and informed consent to the use of the facial recognition technology by the students, since it is included in the competition of the offer, as required by article 1262 of the Civil Code (...).*

Well, this Authority does not question that facial recognition can be an ideal tool in order to ensure that the individual being examined is the same person as the one who enrolled for specific studies. However, for the purposes of assessing whether the adoption of the measure is proportionate, taking into account the purpose of the contract concluded with the student, it is not superfluous to point out that STC 207/1993 provided that, in order to check whether a measure is restrictive of a fundamental right, it must pass the judgment of proportionality, defined in the following terms: " *it is necessary to verify if it meets the three following requirements or conditions: "if such a measure is likely to achieve the proposed objective (juicio de suitability); if, in addition, it is necessary, in the sense that there is no other more moderate measure for the achievement of such a purpose with equal effectiveness (judgment of necessity); and, finally, if it is weighted or balanced, it can be derived of it more benefits or advantages for the general interest than damages on other goods or values in conflict (proportionality judgment in the strict sense)".*

In accordance with this, it must be affirmed that, although the facial recognition system can be an effective tool to control and prevent academic fraud, the truth is that this system does not comply with the principle of legality of treatment imposed by the regulations of data

protection, and that there are other legal measures that are less intrusive and equally suitable for the prevention of academic fraud, when, according to the statements of the FUOC, of the 75,024 students enrolled in the first semester of the 2021-2022 academic year , only 31,501 were submitted to the facial recognition tool - prior to 5th -, and the facial recognition system began to be used on 08/01/2022.

Along these lines, Opinion 6/2014, of Group 29, argues that, in order to assess the "necessity" of the treatment, it is necessary to take into account whether other less invasive means are available that serve the same purpose, as well how to determine if the contract can be executed without this specific treatment (Opinion 6/2014 of Group 29). And, as we have seen, in the present case, the accused entity could use other means to evaluate students, as it had been doing until it launched the facial recognition tool.

In addition, given that the implementation of facial recognition technology is framed in a context characterized by the absence of a rule with the rank of law that establishes the legality requirements of this type of treatment, it is not plausible to affirm the measure adopted by the FUOC – the use of the facial recognition system – exceeds the judgment of proportionality, in the sense that its implementation results in more benefits than harm to the general interest.

The FUOC also invokes, as a legitimizing basis for conducting final assessment tests using a facial recognition system, the University's legitimate interest in preventing student impersonation and fraud in the assessment process -in line with Recital 47 of the RGPD-, as well as the legitimate interest of all students to be evaluated under equal conditions, preventing academic fraud.

Article 6.1 f) of the RGPD determines that the treatment will be lawful if this is *" necessary for the satisfaction of legitimate interests pursued by the person responsible for the treatment or by a third party, provided that these interests do not prevail over fundamental rights and freedoms of the interested party that require the protection of personal data, in particular when the interested party is a child. The provisions in letter f) of the first paragraph will not apply to the treatment carried out by public authorities in the exercise of their functions".*

In relation to this precept, recital 47 of the RGPD establishes: " *The legitimate interest of a person responsible for the treatment, including that of a person responsible to whom personal data may be communicated, or of a third party, may constitute a legal basis for the treatment, as long as the interests or rights and freedoms of the interested party do not prevail, taking into account the reasonable expectations of the interested parties based on their relationship with the person in charge. Such a legitimate interest could arise, for example, when there is a relevant and appropriate relationship between the interested party and the controller, such as in situations where the interested party is a customer or is at the service of the controller. In any case, the existence of a legitimate interest would require a meticulous evaluation, including whether an interested party can reasonably foresee, at the time and in the context of the collection of personal data, that the treatment for that purpose may occur. In particular, the interests and fundamental rights of the interested party could prevail over the interests of the person in charge of the treatment when processing personal data in circumstances where the interested party does not reasonably expect further treatment to be carried out. Since it is up to the legislator to establish by law the legal basis for the treatment of personal data by public authorities , this legal basis should not apply to*

the treatment carried out by public authorities in the exercise of their functions. The processing of personal data strictly necessary for the prevention of fraud also constitutes a legitimate interest of the controller in question. The processing of personal data for direct marketing purposes can be considered carried out for legitimate interest."

In this regard, Opinion 06/14, of the Article 29 Group, includes several elements that can be taken into consideration in order to make the weighting required by Article 6.1 f) RGPD. Among others, the said opinion alludes to the nature of the data, and the impact that the treatment may have on the rights of the persons concerned. And, as has been said, it must be concluded that, given the nature of the data, the intrusion into private life, as well as the impact on the right to data protection of students who must be registered in the facial recognition tool, it is necessary to discard the concurrence of the legitimizing basis of article 6.1.f) RGPD.

On the other hand, evidence that Recital 47 RGPD provides that the processing of personal data must be " *strictly necessary* " for the prevention of fraud, for the purposes of constituting a legitimate interest of the data controller. However, as has already been argued, it can hardly be maintained that facial recognition is strictly necessary to control student impersonation, when there are other formulas that lead to the same result.

2.2. Alternative to the processing of biometric data for the verification of student identity

In the proposed resolution, the instructor suggested urging the FUOC to " *adopt measures to ensure that the students who have to take these assessment tests can choose freely and voluntarily between taking the tests using the facial recognition tool, or by means of any other alternative system that is not particularly burdensome to them and that respects current legislation on data protection. In this sense, for the purposes of considering that the students have given their explicit consent to submit to the facial recognition tool, they must be clearly informed that the choice of the evaluation system will not entail any discrimination nor will it affect in any way its evaluation".*

Well, in relation to this point, the FUOC in its statement of objections to the proposed resolution suggests two alternatives for the purposes of correcting the infringement, which will be analyzed in the 5th legal basis of this resolution.

2.3. In relation to the alleged lack of prejudice to the persons concerned

The accused entity reiterates the arguments collected in the written documents previously presented to the Authority , when it maintains that the use of the facial recognition system has not caused any harm to the students enrolled in the studies that required this evaluation system since, in all moment, students are aware of the use that the University will make of their personal data. Likewise, it states that this is a *"transparent, informed and documented" treatment* and that students are offered the possibility to exercise any of the rights provided for in the regulations for the protection of personal data, as well as to contact the representative of protection of personal data.

In relation to the above, this Authority does not share the arguments of the accused entity since it cannot be affirmed in a reliable way that the lack of damage to the students who have been subjected to a facial recognition system. In this regard, it should be borne in mind that

some students have complained to this Authority about the controversial treatment, as well as the fact that the FUOC does not offer the possibility of evaluating students through an alternative system to facial recognition, which is in accordance with the RGPD and the LOPDGDD. And, in relation to the above, it is necessary to add the consequence of not consenting to the aforementioned treatment, which has been associated with obtaining the qualification of "Not submitted".

In any case, it should be noted that the existence or lack of damages is not an element required by the infringing type applied, to consider the infringement committed.

2.4. In relation to the presumed absence of guilt

The accused entity highlights the lack of intentionality and culpability, in relation to the facts that are the subject of this procedure. Likewise, in relation to the principle of culpability, he invokes the sentence number 76/1990, of April 26, of the Constitutional Court, according to which, the principles and guarantees present in the field of Criminal Law are applicable , with certain nuances, to the exercise of any sanctioning power of the Public Administration.

Likewise, the FUOC also cites the judgment of February 10, 1986 of the Supreme Court which establishes the following:

> *"the exercise of punitive power, in any of its manifestations, must be accommodated to the constitutional principles and precepts that preside over the criminal legal system as a whole, and, whatever it may be, the sphere in which the punitive power of the State, the Jurisdiction, or the field in which it occurs, is subject to the same principles whose respect legitimizes the imposition of penalties and sanctions, therefore, administrative infractions, to be subject to sanctions or penalties, must be typical, that is to say, provided as such by a previous legal norm, anti-legal, that is, harmful to a legal good provided for by the Ordinance, and culpable, attributable to an author by reason of dolo or fault, to ensure in its assessment the balance between the interest public and the guarantee of the people which is what constitutes the key to the Rule of Law".*

Finally, in its statement of objections to the proposed resolution, the FUOC concludes that, " *considering that the processing of data that is the subject of this procedure has been adjusted to the Law, based on grounds of legitimacy not disputed by this Authority and having incorporated proposals for alternative identity verification mechanisms for interested parties who do not wish to be subject to the aforementioned treatment, it is appropriate to estimate the total absence of guilt".*

In this regard, first of all, it should be pointed out that, contrary to what the FUOC argues, this Authority did disagree on the legal bases invoked by the entity and which, in its opinion, legitimized the processing of biometric data (paragraph 2 of the 2nd legal basis of this resolution).

On the other hand, the concurrence of the culpability element, that is to say, the need for there to be grief or guilt in the punitive action, is fully applicable to the penal administrative law, in accordance with what is provided for in article 28 of Law 40/2015, of 1 October, on the legal regime of the public sector. This need for guilt as a constitutive element of the

administrative offense has been expressly recognized by the Constitutional Court, in ruling 76/1990, invoked by the FUOC.

Having said that, it must be stated that the implementation of a facial recognition system, for the purpose of assessing students' knowledge, is not a conduct that obeys an involuntary oversight but that the FUOC carried out the controversial treatment deliberately and consciously Consequently, the fact that she acted with the conviction that she was complying with the provisions of the current data protection regulations, does not fit into an assumption of lack of guilt, which allows her to be exonerated from responsibility.

3. In relation to the facts described in the proven facts section, relating to the use of the facial recognition system for the performance of final evaluation tests, it is necessary to refer to article 5.1 a) of the RGPD , which provides that personal data will be *" treated in a lawful, fair and transparent manner in relation to the interested party ("legality, loyalty and transparency").*

In this sense, the RGPD provides that all processing of personal data must be lawful (article 5.1 a) and, in relation to this, establishes a system for legitimizing the processing of data which is based on the need for some of the legal bases established in its article 6.1, previously transcribed.

For its part, article 9.1 of the RGPD, also transcribed, provides for the prohibition of treating special categories of personal data (among them, biometric data aimed at uniquely identifying a natural person), not concurrent in the case present none of the exceptions provided for in section 2 of said precept, which would lift this prohibition.

During the processing of this procedure, the fact described in the section on proven facts has been duly proven, which is constitutive of the violation provided for in article 83.5.a) of the RGPD, which typifies the violation of "the *principles básicos para el tratamiento, including the conditions for consent pursuant to articles 5,6, 7 and 9 ",* among which is the principle of legality (article 5.1 a) in relation to article 9 RGPD.

The conduct addressed here has been included as a very serious infraction in article 72.1.e) of the 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. When the FUOC does not fit into any of the subjects provided for in article 77.1 of the LOPDGDD , the general sanctioning regime provided for in article 83 of the GDPR applies.

Article 83.5 of the RGPD provides for the infractions provided for there, to be sanctioned with an administrative fine of 20,000,000 euros at most, or in the case of a company, an amount equivalent to 4% as a maximum of the global total annual business volume of the previous financial year, opting for the higher amount.

Having said that, it is necessary to determine the amount of the administrative fine to be imposed. According to what is established in article 83.2 of the RGPD, and also in

accordance with the principle of proportionality enshrined in article 29 of Law 40/2015, as indicated by the instructing person in the proposed resolution, the penalty of 20,000 euros (twenty thousand euros). This quantification of the fine is based on the weighting between the aggravating and mitigating criteria indicated below.

As mitigating criteria, the concurrence of the following causes is observed:

- The carrying out of an impact assessment by the FUOC in relation to the controversial treatments (83.2.k RGPD)
- The lack of benefits obtained as a result of the infringement (art. 83.2.k RGPD and art. 76.2.c LOPDGDD)

On the contrary, as aggravating criteria, the following elements must be taken into account :

- The nature, severity and duration of the infringement, as well as the number of people affected (art. 83.2 GDPR). It follows from the alleged facts that, at least on 04/11/2022, 31,501 students have been subjected to the facial recognition system to be evaluated, and that the data that has been collected from these people includes within the classification of special categories, in accordance with article 9.1 RGPD.
- Linking the offender's activity with the practice of processing personal data (art. 83.2 b RGPD). To the extent that the accused entity is a University, it must be affirmed that there is a close link between its educational activity and the processing of a considerable amount of personal data - not only of undergraduate or postgraduate students, but also of 'researchers and researchers, and other personnel who can provide their services to the entity -.
- The categories of personal data affected by the infringement (art. 83.2 g RGPD)
- The sanctions imposed by this Authority on the entity accused of breaching data protection legislation, prior to the alleged events (art. 83.2 e RGPD) – sanctioning procedures no. PS 40/2014, PS 29/2017, and PS 27/2021.
- The continuing nature of the offense (art. 76.2 b LOPDGDD)

Finally, it should be noted that the accused entity, in its statement of objections to the proposed resolution, requests the reduction of the amount of the fine proposed by the instructor of the procedure. In literal terms, the imputed entity declares the following:

> "That, *in the event that this Authority considers that it must sanction the FUOC, take into consideration the proposed measures, applying the sanction in the first half of the lower part".*

However, neither the RGPD, nor the LOPDGDD, consider as mitigating the fact that, within the framework of a sanctioning procedure, the accused entity proposes the adoption of certain corrective measures in order to prevent further violations the data protection regulations, in fact, the obligation of everyone responsible for the treatment is to avoid violating said regulations. The fulfillment of an obligation cannot, therefore, be considered a mitigating factor, which is why the application of the reduction requested by the FUOC must be discarded.

5. Given the findings of the violations provided for in art. 83 of the RGPD in relation to privately owned files or treatments, article 21.3 of Law 32/2010, of October 1, of the Catalan Data Protection Authority, empowers the director of the Authority for the resolution declaring

the infringement to establish the appropriate measures so that its effects cease or are corrected.

The person instructing this procedure proposed requiring the FUOC to adopt measures to ensure that students can choose freely and voluntarily between taking the tests using the facial recognition tool, or using any other alternative system that does not is particularly burdensome and that respects current data protection regulations. So, for the purposes of considering that the students have given their explicit consent to submit to the facial recognition tool, the proposed resolution argued that the FUOC had to clearly inform that the choice of the evaluation system it will not involve any discrimination or affect in any way its evaluation.

In this regard, the accused entity, in the allegations in the resolution proposal, suggests, in addition to providing the students with the pre-contractual information contained in both the general conditions of employment, as well as in the academic regulations and the policy of privacy, " *further strengthen this pre-contractual information through the incorporation in the process of formalizing the registration of a specific notice regarding the treatment of biometric data in order to verify the identity of the students during the final evaluation process as necessary element of the contract, as well as the impossibility of continuing with its formalization in case of disagreement. In other words, a potential student who disagrees with the methodologies used by the FUOC can freely and in an informed manner, decide not to enroll there by virtue of exercising his right to choose a university center."*

The FUOC explains that this alternative includes the following actions:

(i) " *Strengthen communication prior to the registration process. Include information relating to the identification methods used by the FUOC in the pre-contractual phase , including advertising material for the services offered by the University.*

(ii) *Strengthen communication during the registration process. Incorporation in the process of formalizing the registration of a specific notice regarding the processing of biometric data with the purpose of verifying the identity of the students during the final evaluation process as a necessary element of the recruitment.*
By way of example, the informative notice could have the following text: "Choosing the UOC as a university to start or continue your university studies and, therefore, to enroll in this University, implies that, in the subjects for which there is an assessment test, facial recognition tools will be used with biometric techniques to prevent impersonation and academic fraud. If you do not agree, it will not be possible to continue with the registration process".

(iii) *Impossibility to continue with the formalization of the registration, in case of disagreement with the use by the FUOC of the reported data processing".*

Next, the accused entity suggests, as a subsidiary measure in the event that this Authority does not consider the first measure proposed to be in accordance with the law, the creation of a specific procedure to convey the possibility that those students who so wish, can opt for an alternative mechanism. In this case, the proposed alternative would include the following:

(i) *Strengthen communication prior to the enrollment process. Include information relating to the identification methods used by the UOC in the pre-contractual phase , including advertising material for the services offered by the University.*

(ii) *Create a specific procedure to ensure that students who do not wish the UOC to carry out the processing of biometric data for the verification of their identity, access an alternative mechanism.*
The mechanisms foreseen will, as a general rule, be face-to-face assessment or synchronous oral assessment, since these are the ways that could equal the guarantees offered by identification through facial recognition. The selection of one of these two mechanisms, or another as the case may be, will be determined by the University based on teaching criteria.

(iii) *Reinforce communication after the registration process, include information about the specific procedure that enables the alternative to the use of biometric data for those students who wish to do so.*

In this regard, it should be pointed out that the first alternative proposed by the accused entity involves making registration conditional on the acceptance of the processing of the student's personal data, using the facial recognition tool. A proposal that does not conform to the measure proposed by the instructor of the procedure given that it does not correct the effects of the infringement, nor does it respect the data protection regulations, for the reasons that will be set out below.

Precisely the facts that are imputed in the present procedure are constitutive of an infringement given that participation in assessment tests is conditioned on the processing of the students' personal data, through the facial recognition tool, without students have an alternative to the processing of their biometric data, in order to take the assessment tests. Therefore, making enrollment conditional on the acceptance of the controversial treatment also contravenes the data protection regulations, to the extent that the students also do not have an alternative mechanism to the controversial data treatment, in order to be able pursue the desired studies.

The second alternative proposed by the FUOC, as a corrective measure for the effects of the offense charged here, is to strengthen the information that is provided to students before and after they enroll, to create a specific procedure for those students who refuse to submit to the facial recognition tool, and offer them the option of being assessed face-to-face or through "synchronous oral assessment".

This second proposal from the FUOC is in line with the one proposed by the instructor of this procedure, insofar as it offers students alternatives to the facial recognition system to be assessed, face-to-face assistance or a synchronous oral assessment, in it is well understood that the synchronous oral assessment cannot involve the processing of biometric data intended to uniquely identify a physical person, and that students who refuse to submit to the facial recognition system, so that the alternative system does not work for them particularly burdensome , they must be able to choose delivery between one of these two options proposed by the FUOC. Likewise, and with respect to students who agree to be evaluated using the facial recognition tool, the FUOC will have to collect their explicit consent for the processing of their biometric data.

In view of the above, the FUOC should be required to offer its students a double alternative to the facial recognition system in order to carry out the assessment tests, that is to say, they can freely choose between a face-to-face assistance system or a synchronous oral assessment that does not involve the processing of biometric data, and collecting in any case the explicit consent of those students who opt for the facial recognition system to be evaluated.

Once the corrective measures described in the previous paragraph have been adopted within the period indicated, within the next 10 days the FUOC must inform the Authority, without prejudice to the Authority's inspection powers to carry out the corresponding checks.

For all this, I resolve:

1. To impose on the Foundation for the Open University of Catalonia the sanction consisting of a fine of 20,000.- euros (twenty thousand euros), as responsible for an infringement provided for in article 83.5.a) in relation to the article 5.1 a) and 9, both of the RGPD.

2. fine legal basis , and to accredit before this Authority the actions carried out to comply with them.

3. Notify this resolution to the Foundation for the Open University of Catalonia.

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,