

Identificación del expediente

Resolución de procedimiento sancionador núm. PS 41/2022, referente a la Fundación para la Universidad Oberta de Catalunya

Antecedentes

1. En fecha 04/11/2021, tuvo entrada en la Autoridad Catalana de Protección de Datos un escrito de una persona por el que formulaba denuncia contra la Fundación para la Universidad Abierta de Cataluña (en adelante, FUOC) con motivo de un presunto incumplimiento de la normativa de protección de datos.

En concreto, la persona denunciante exponía que desde la FUOC se estaría empleando una herramienta de reconocimiento facial para comprobar la identidad de los y las estudiantes durante la realización de pruebas de evaluación a distancia. Al respecto, exponía que el funcionamiento de este sistema requiere, en primer lugar, que el estudiante capture una imagen de su rostro, a fin de que la herramienta pueda compararla con su fotografía de DNI, y verificar que es la persona quien dice ser. Asimismo, la fotografía también servía para compararla con las imágenes que se capturan mientras el estudiante realiza la prueba de evaluación a distancia, a efectos de verificar la identidad del alumnado. A continuación, la persona denunciante exponía que es obligatorio el registro en la herramienta de reconocimiento facial para poder realizar las pruebas de evaluación.

Con el fin de acreditar los hechos denunciados, aportaba diversa información, entre la que destaca un correo electrónico que la FUOC le habría enviado en fecha 04/11/2021, cuyo asunto se refería a " Pruebas virtuales: haz el registro en la herramienta de reconocimiento facial ". Mediante el referido correo electrónico, se informaba a la persona denunciante que podía proceder a registrarse en la herramienta de reconocimiento facial, para poder validar su identidad " mientras hagas las pruebas ". Igualmente, se le informaba que " la aplicación captará una serie de fotografías y las comparará con la fotografía del documento de identidad que nos hayas hecho legar previamente para garantizar que eres tú. Estas imágenes se compararán con las que capturemos mientras hagas las pruebas finales. Por este motivo, este paso es imprescindible para poder realizar las pruebas finales ".

A esa denuncia se le asignó el núm. IP 448/2021.

2 . En fechas 16/11/2021, 01/12/2021, 27/04/2021 y 02/05/2022, cuatro personas más presentaron, respectivamente, cuatro escritos mediante los cuales denunciaban estos mismos hechos relacionados con la utilización por parte de la FUOC de la herramienta de reconocimiento facial en las pruebas de evaluación.

A estas denuncias se les asignó los siguientes números: IP 469/2021, IP 489/2021, IP 150/2022 e IP 158/2022, respectivamente.

3. La Autoridad abrió una fase de información previa, de acuerdo con lo que prevé el artículo 7 del Decreto 278/1993, de 9 de noviembre, sobre el procedimiento sancionador de aplicación a los ámbitos de competencia de la Generalidad , y el artículo 55.2 de la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las administraciones

públicas (en adelante, LPAC), para determinar si los hechos eran susceptibles de motivar la incoación de un procedimiento Sancionador.

4. En esta fase de información, en fecha 03/05/2022 la Autoridad requirió a la entidad denunciada para que informara, entre otras cuestiones, sobre la base jurídica que legitimaría el uso de un sistema de reconocimiento facial para evaluar a los estudiantes, para que argumentara la circunstancia que habilitaría el tratamiento de categorías especiales de datos personales, para que señalara si se ofrecía al alumnado la posibilidad de realizar las pruebas a distancia por medio de otro sistema alternativo al reconocimiento facial, y para que indicara qué consecuencias tendría el alumnado que decidiera no registrarse en la herramienta del reconocimiento facial.

5. En fecha 16/05/2022, la FUOC respondió el requerimiento mencionado a través de escrito en el que exponía lo siguiente:

- “ Las bases jurídicas que legitiman la implementación de este tratamiento de datos personales son dos. Por un lado, la ejecución del contrato (verificar la identidad de la persona que realiza la prueba final de evaluación –en adelante, “PAF”-) y, por otro, el interés legítimo en prevenir y detectar el fraude académico. El tratamiento consistente en la verificación de la identidad de las personas que realizan la PAF es parte esencial en el contrato de prestación de servicios académicos, formalizado entre el estudiante y nuestra universidad, es decir, la matrícula. Por tanto, la base jurídica que legitima la verificación de la presencia de las partes del contrato (matrícula) en el momento esencial de la relación contractual, como es la verificación de los conocimientos (prueba final), es la ejecución del contrato.

- El tratamiento consistente en la prevención y detección del fraude se basa en el interés legítimo, de acuerdo con lo que se establece en las propias directrices 2/2019 del CEPD. La UOC realizó la correspondiente ponderación del interés legítimo y dispone de las evidencias de esta ponderación.

- La UOC no ha aplicado en este tratamiento de datos personales la base jurídica del consentimiento ya que, según doctrina del CEPD y de la propia APDcat, existe el riesgo de que el consentimiento no se considere libremente prestado en este caso.

- Las enseñanzas que imparte la Universidad son en modalidad docente virtual (no presencial) y que la evaluación se realiza, con carácter general, de forma virtual, utilizando herramientas de verificación de identidad en los casos de evaluación mediante PAF. Esta información llega al estudiante antes de la frase pre -contractual, en el momento en que recopila la información sobre el programa formativo que quiere cursar y, por tanto, cuando adopta la decisión de realizarla, ya conoce el sistema de verificación, tanto de los conocimientos como de la identidad, que se utilizará la Universidad (...). Por tanto, el estudiante es consciente y libre a la hora de escoger una Universidad y unos estudios que se ajusten a sus necesidades”.

La FUOC también señalaba que el sistema de evaluación del proceso de aprendizaje de los estudiantes de cada asignatura se establece semestralmente en el plan docente correspondiente, argumentando que se limitan el número de asignaturas que se evalúan mediante PAF y que, tanto, requerirán de verificación de identidad. Asimismo, exponía que la falta de identificación de la persona que se presenta en una PAF online en el marco del contrato de prestación de servicios académicos supone que conste en su expediente académico la calificación final de “No presentado”. Y añadía a continuación:

- *Al amparo de lo establecido en la Normativa de Derechos y Deberes de la UOC, que consta publicada en la Sede Electrónica de la Universidad, la Universidad también contempla supuestos en los que los estudiantes con necesidades especiales, o bien, con circunstancias personales que, debidamente acreditadas, justificarían una adaptación curricular y la posibilidad de poder realizar una PAF sin verificación de su identidad (...). Los supuestos que posibilitan la realización de las PAF adaptadas son los que se contemplan en el documento que se adjunta como Anexo 3.*
- *La normativa interna de la Universidad también prevé la posibilidad de que el estudiante justifique la necesidad de realizar la prueba sin utilizar la herramienta de reconocimiento facial para la verificación de su identidad. En tal caso, la verificación de la identidad del estudiante se realiza de forma manual.*
- *La primera PAF online en la que se empleó el sistema de reconocimiento facial para la realización de pruebas online tuvo lugar el día 8 de enero de 2022 (...).*
- *De un total de 75.024 estudiantes matriculados en el primer semestre del curso académico 2021-2022, sólo 31.501 estudiantes han realizado PAF con autenticación de identidad.*

La entidad denunciada adjuntaba en el escrito documentación diversa. Entre esta información, aportaba la Normativa de Derechos y Deberes de la FUOC que contempla que quedan exentos de la comprobación de la identidad a través de fotografías las siguientes personas: "a) personas ciegas o con discapacidad visual grave b) personas con trastornos mentales c) personas con problemas graves de movilidad".

6. En fecha 14/06/2022, la directora de la Autoridad Catalana de Protección de Datos acordó iniciar un procedimiento sancionador contra la FUOC por una presunta infracción prevista en el artículo 83.5 a) en relación con el artículo 5.1 a); todos ellos del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril, relativo a la protección de las personas físicas en lo que se refiere al tratamiento de datos personales ya la libre circulación de éstas (en adelante, RGPD). Este acuerdo de iniciación se notificó a la entidad imputada en fecha 16/06/2022.

7. En fecha 17/06/2022, la FUOC presentó una solicitud de ampliación del plazo otorgado para la presentación de alegaciones en el acuerdo de iniciación señalado en el antecedente anterior.

8. En fecha 28/06/2022, la instructora del procedimiento acordó la ampliación del plazo solicitado por la FUOC, al amparo del artículo 32 de la LPAC.

9. En fecha 08/07/2022 la entidad imputada formuló alegaciones al acuerdo de iniciación, aportando con su escrito documentación diversa.

10. En fecha 13/10/2022 la FUOC presentó un escrito mediante el cual ampliaba las alegaciones formuladas el 08/07/2022, aportando la documentación que se relaciona a continuación, la cual habría sido adaptada como consecuencia de la implementación del sistema de reconocimiento facial en la realización de las pruebas de evaluación final, y esto " a efectos de evidenciar que la FUOC actúa con la diligencia debida, como garante de los derechos académicos de sus estudiantes ":

- *“Texto del formulario de matrícula actual.*
- *Texto de las Condiciones Generales de Contratación vigente.*
- *Texto de la Normativa Académica de la UOC vigente.*
- *Texto de la política de privacidad de la UOC vigente.*
- *Esquema de las principales acciones de comunicación dirigidas a los y las estudiantes en relación a las pruebas de evaluación finales y el uso de sistemas de reconocimiento facial, y algunos ejemplos de dichas comunicaciones”.*

11. En fecha 04/11/2022, la instructora de este procedimiento formuló una propuesta de resolución, por la que proponía que la directora de la Autoritat Catalana de Protecció de Dades impusiera a la FUOC una multa de 20.000 euros (veinte -mil euros) como responsable de una infracción prevista en el artículo 83.5.a) en relación con los artículos 5.1.a) y 9; todos ellos del RGPD.

Esta propuesta de resolución se notificó en fecha 04/11/2022 y se concedía un plazo de 10 días para formular alegaciones.

12. En fecha 10/11/2022 la FUOC presentó una solicitud de ampliación del plazo otorgado para la presentación de alegaciones en la propuesta de resolución.

13. En fecha 11/11/2022, la instructora del procedimiento acordó la ampliación del plazo solicitado por la FUOC.

14. En fecha 25/11/2022, la entidad imputada presentó un escrito de alegaciones a la propuesta de resolución, que se abordan en los fundamentos de derecho 2º y 5º de esta resolución.

Hechos probados

Desde el 08/01/2022, fecha en que por primera vez la Fundació para la Universitat Oberta de Catalunya empleó el sistema de reconocimiento facial para la realización de pruebas online, y hasta el 16/05/2022, se han examinado un total de 31.501 estudiantes utilizando la citada herramienta a efectos de validar su identidad mientras tanto realizaban las pruebas de evaluación a distancia. Al respecto, cabe señalar que la FUOC advertía a los y las estudiantes que el registro en la herramienta de reconocimiento facial era imprescindible a los efectos de poder realizar la prueba de evaluación y que, de no registrarse, se obtendría la calificación final de " *No presentado*".

Fundamentos de derecho

1. Son de aplicación a este procedimiento lo que prevén la LPAC , y el artículo 15 del Decreto 278/1993, según lo que prevé la DT 2a de la Ley 32/2010, de 1 de octubre, de Autoritat Catalana de Protecció de Dades. De conformidad con los artículos 5 y 8 de la Ley 32/2010, la resolución del procedimiento sancionador corresponde a la directora de la Autoritat Catalana de Protecció de Dades.

2. La entidad imputada ha formulado alegaciones a la propuesta de resolución, en la que, en esencia, reitera aquellas que formuló en el acuerdo de iniciación, y que a continuación se analizan.

2.1. Sobre la naturaleza de datos biométricos y sobre las bases legitimadoras del tratamiento.

En esencia, la FUOC centra el primer punto de sus alegaciones en argumentar que, por un lado, los datos biométricos que utiliza para verificar la identidad de los estudiantes, en el marco de las pruebas de evaluación final, no son categorías especiales de datos, y por otra parte, que las bases jurídicas que legitiman el uso de los datos biométricos son la ejecución de un contrato - la matrícula universitaria - y el interés legítimo.

2.1.1. Sobre el carácter de categoría especial de los datos biométricos empleados para la verificación de la identidad del alumnado en el marco de las pruebas de evaluación.

A efectos de analizar e interpretar el artículo 9 RGPD, en relación con el artículo 4.1.14 RGPD, a continuación se reproduce el contenido de estos preceptos.

Artículo 4 *Definiciones*

1.14) «datos biométricos»: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirman la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos;

Artículo 9 *Tratamiento de categorías especiales de datos personales*

1. Quedan prohibidos el tratamiento de datos personales que revelan el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de forma unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física.

2. El apartado 1 no será de aplicación cuando concurra una de las siguientes circunstancias:

- a) el interesado dio su consentimiento explícito para el tratamiento de dichas datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;*
- b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo conforme al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;*
- c) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento;*
- d) el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin*

ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que las datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados;

e) el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos;

f) el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial;

g) el tratamiento es necesario por razones de un interés público esencial, en base al Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;

h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3;

i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, en base al Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional,

j) el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, en base al Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

3. Las datos personales a que se refiere el apartado 1 podrán tratarse en los fines citados en el apartado 2, letra h), cuando su tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con el Derecho de la Unión o de los Estados miembros o con las normas establecidas por los organismos nacionales competentes, o por cualquier otra persona sujeta también a la obligación de secreto de acuerdo con el Derecho de la Unión o de los Estados miembros o de las normas establecidas por los organismos nacionales competentes.

4. Los Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones, respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud.

Como se ha avanzado, en su escrito de alegaciones a la propuesta, la entidad imputada reitera la argumentación recogida en las alegaciones en el acuerdo de iniciación de este procedimiento, defendiendo la existencia de dos tipologías de datos biométricos. Por una parte, aquellas que se dirigen a identificar de forma unívoca a una persona y, por otra parte, aquellas que no tienen la consideración de datos especialmente protegidos – como la voz o una fotografía – que se dirigen a autenticar la identidad de un individuo. Al respecto, la

FUOC sostiene que el tratamiento de datos personales mediante el reconocimiento facial, en la medida en que verifica la identidad del alumnado, y no se dirige a identificarlo unívocamente, no constituye un tratamiento de categorías especiales de datos. En esta línea, la entidad imputada defiende que la diferenciación entre las dos tipologías de datos biométricas se fundamenta en criterios ajustados a Derecho y compartidos por el Comité Europeo de Protección de Datos, por el Dictamen 3/2012 emitido por el Grupo de Trabajo del artículo 29, y por el Informe 0036/2020 de la Agencia Española de Protección de Datos Personales (en adelante, AEPD), entre otros.

En relación con lo anterior, en la propuesta de resolución se argumentaba que, el Dictamen 3/2012 emitido por el Grupo de Trabajo del artículo 29, es anterior a la entrada en vigor del RGPD y, por tanto, se lleva a cabo en un contexto en el que el concepto de dato biométrico no se da dentro de la consideración de categoría especial de datos, lo que, en la actualidad, no resultaría, en ningún caso admisible, a la luz de la definición de dato biométrico, previsto en el artículo 4.14 RGPD. Y, al respecto, la FUOC, en su escrito de alegaciones a la propuesta de resolución, defiende lo siguiente:

“El hecho de que éste fecha del año 2012 (efectivamente, antes de la entrada en vigor del RGPD) no invalida, ni contradice sus consideraciones. Prueba de ello, es que este Dictamen fue tomado en consideración por la Agencia Española de Protección de Datos en su Informe 0036/2020.

Asimismo, existen pronunciamientos posteriores a la entrada en vigor del RGPD que sustentan la misma interpretación.

Ponemos de especial atención en estos:

- *Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. Se identifica claramente la categoría especial del dato en caso de que esté dirigida a la identificación unívoca.
Preámbulo : Apartado IV (...) Las datos biométricos (como las huellas dactilares o la imagen facial) sólo se consideran incluidas en esta categoría especial cuando su tratamiento está dirigido a identificar de forma unívoca a una persona física. (...)
Artículo 13. Tratamiento de categorías especiales de datos personales. (...)*
- *Directrices 3/2019 sobre el tratamiento de datos personales mediante dispositivos de vídeo, del CEPD. Versión 2.0 Adoptadas el 29 de enero de 2020: se aborda especialmente la diferencia entre sí los datos los han tratado técnicamente de forma específica para contribuir a la identificación unívoca de una persona (...)*
- *Directrices 2/2021 sobre los asistentes de voz virtuales del CEPD, versió 2.0 Adoptadas el 7 de julio de 2021. (...)*

Por todo lo expuesto, el criterio consistente en distinguir la identificación de la autenticación, mencionado en el Dictamen 3/2012, sigue siendo plenamente válido, con independencia de la entrada en vigor del RGPD, existiendo una voluntad legislativa de hacer esta distinción”

En relación con lo anterior, la FUOC argumenta que, sostener que su interpretación no es válida, genera indefensión jurídica fruto de la discrepancia o carencia de criterio unitario entre diferentes autoridades de control y que “ requeriría de las acciones necesarias para la unificación criterios y la obtención de un pronunciamiento único y coherente”.

Al respecto, cabe reiterar aquí lo que la instructora argumentó en la propuesta de resolución, poniendo de manifiesto que, a tenor del artículo 9.1 del RGPD, se prohíbe el tratamiento de los datos biométricos dirigidos a identificar o autenticar una persona, salvo que concurra alguna de las excepciones previstas en el apartado 2 del mismo precepto. También cabe citar el Considerante 51 del RGPD, que especifica que “ (...) *el tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física. (...)*”

Esta Autoridad no puede compartir la interpretación de la entidad imputada, que sostiene que la verificación o autenticación de una persona mediante reconocimiento facial no constituye un dato biométrico de categoría especial, en los términos establecidos por el artículo 9 RGPD. El criterio de esta Autoridad, plasmado en su Dictamen CNS 21/2020, está claro cuando sostiene que el artículo 9 del RGPD, cuando se refiere a la identificación unívoca de una persona, incluye los conceptos de “autenticación o verificación”, puesto que tanto la autenticación como la verificación permiten la identificación única de una persona. En términos literales, el citado Dictamen argumenta lo siguiente:

“(...) no parecería conveniente excluir una parte de los datos biométricos (aquellos que se someten a un tratamiento técnico específico con el fin de verificar la identidad de una persona) de la protección reforzada que el RGPD reconoce a aquellos datos personales que por su naturaleza y el contexto en que se tratan, se convierten en particularmente sensibles, en atención a las consecuencias que, para las personas afectadas, pueden derivarse de su tratamiento, lo que tendría lugar si no se las reconociera como a categoría especial de datos.

No puede obviarse que la identificación y la autenticación, a pesar de responder a objetivos diferentes, son conceptos estrechamente vinculados entre sí.

Con la identificación se pretende determinar la identidad (reconocer) de una persona (¿quién eres?) a partir, en este caso, de sus características físicas, fisiológicas o conductuales. Con la autenticación se pretende utilizar estos datos para confirmar o desmentir la identidad de esa persona (¿eres quien dices ser?) y esta actuación implicaría, en todo caso, haber identificado antes a esa persona.

Cuando se hace una autenticación, por ejemplo cuando se identifica a una persona mediante la huella al entrar en el trabajo, en algunos casos conlleva una identificación uno a uno (por ejemplo, si paralelamente se emplea una tarjeta de marcado o uno código para identificarse) o puede operar como un sistema de correspondencia uno a varios (por ejemplo si la huella del trabajador que accede al puesto de trabajo se compara con la de todos los trabajadores de la empresa para terminar determinando quién es el trabajador que ha accedido).

Hay que interpretar que, cuando el RGPD se refiere a la identificación unívoca de una persona física en el artículo 9.1, también está haciendo referencia a la autenticación de la identidad de esa persona (“confirmar”).

Respecto al hecho de que otras autoridades – como la Agencia Española de Protección de Datos – hayan defendido la existencia de dos tipologías de datos biométricos, no condiciona el criterio de esta Autoridad, ni el sentido de la presente resolución, en la medida que no está sujeta a los criterios interpretativos de otras autoridades de control, respecto de las cuales no existe una relación de subordinación.

En relación con lo anterior, la FUOC arguye que la falta “ *de criterio unitario entre diferentes Autoridades de Control*”, genera indefensión, y ha señalado que deberían llevarse a cabo las acciones necesarias para la unificación de criterios.

Sin embargo, al respecto, la entidad imputada no puede desconocer que, el Informe 0036/2021 de la AEPD, invocado en sus escritos de alegaciones y que, según dice, recoge el criterio del Grupo del artículo 29, a pesar de sostener la existencia de dos categorías de datos biométricos, está claro cuando concluye que, en los procesos de reconocimiento facial empleados para la realización de evaluaciones on-line, el tratamiento de datos biométricos se lleva a cabo con la finalidad de identificar unívocamente a una persona y constituye, por tanto, un tratamiento que se da dentro de las prohibiciones del artículo 9.1 RGPD.

2.1.2. Sobre las bases jurídicas que legitiman el tratamiento de los datos biométricos controvertido.

En su escrito de alegaciones a la propuesta, la entidad imputada da por reproducidos los argumentos jurídicos recogidos en los diferentes escritos presentados ante la Autoridad, en el marco del presente procedimiento, y reitera que, las bases que legitiman el tratamiento son la ejecución de un contrato – con el fin de “*verificar la identidad de la persona que realiza la prueba final de evaluación – en adelante, “PAF”-*” y el interés legítimo –por “*prevenir el fraude académico*”-, previstas, respectivamente, en el artículo 6.1 apartados b) y f) del RGPD.

De acuerdo con el principio de licitud, consagrado en el artículo 5.1 a) del RGPD, los datos personales deben ser tratados “*de forma lícita, leal y transparente en relación con el interesado*”. Así pues, para que un tratamiento de datos de categoría especial – como es el caso – sea lícito, es necesario que concurra una de las bases jurídicas del artículo 6.1 del RGPD, que habilitan el tratamiento de datos personales, así como alguna de las excepciones previstas por el artículo 9.2 del RGPD, que permitan levantar la prohibición general del artículo 9.1 del RGPD.

En primer término hay que evidenciar que la entidad imputada parte de la premisa de que los datos biométricos controvertidos no tienen la condición de categoría especial de datos, por lo que no ha invocado en sus escritos de alegaciones ninguna de las excepciones previstas en el artículo 9.2 RGPD. En todo caso, no se observará que pueda ser de aplicación ninguna de las excepciones recogidas en el referido artículo. Sin embargo, no resulta de más reproducir aquí el análisis efectuado en la propuesta sobre las dos excepciones que, en base a las bases jurídicas del tratamiento invocadas por la FUOC, podrían tener cierta relación con ellas, como sería el consentimiento explícito prestado por la persona afectada, y la concurrencia de un interés público esencial (artículo 9.2 letras a) y g) RGPD, respectivamente).

En cuanto al consentimiento, la propia FUOC reconoció – y así lo manifestó expresamente en el marco de la información previa que precedió a este procedimiento-, no haber basado el tratamiento controvertido en el consentimiento, dado que éste podría no ser libre, y incumplir así uno de los requisitos que, entre otros, debe reunir el consentimiento, por considerarse válidamente prestado (art. 4.11, en conexión con los considerantes 32 y 42 RGPD).

Esta Autoridad comparte el criterio de la entidad imputada que impide considerar que los y las estudiantes puedan consentir libremente el tratamiento de datos controvertido toda vez que, si no aceptan someterse a la herramienta del reconocimiento facial, obtienen la calificación de “No presentado” y, por tanto, no disponen de otra alternativa para realizar las pruebas de evaluación final (salvo alguna excepción muy puntual – antecedente 5º in fine). Y a lo anterior hay que añadir que el consentimiento prestado en caso de que aquí se trata podría no reunir otras condiciones que prevé la normativa, como sea explícito.

Asimismo, sobre la presunta existencia de un interés público esencial – arte. 9.1.g) RGPD –, y en línea con el Dictamen 17/2020 de esta Autoridad, cabe señalar que, cuando el Considerante 41 del RGPD precisa que cuando el Reglamento hace referencia a una base jurídica, no exige necesariamente que ésta se trate de un acto legislativo adoptado por un Parlamento, pero establece que deberá estar en los requisitos que el ordenamiento constitucional del Estado miembro contemple. Y, al respecto, cabe poner de manifiesto que, de acuerdo con el ordenamiento jurídico español, la norma que establezca el tratamiento de datos personales deberá tener rango de ley, en cumplimiento del artículo 53 CE, en la medida en que comporta la limitación de un derecho fundamental, tal y como ha reconocido la jurisprudencia constitucional recogida en el Dictamen 17/2020 de esta Autoridad (SSTC 292/2000, SSTC 76/2019, STJUE 08.04.2014, Digital Rights (Ireland), entre otros).

De acuerdo con lo expuesto, dado que en la actualidad no se dispone de una norma con rango de ley que habilite a las universidades y otros centros docentes para el tratamiento de datos biométricos para este fin (evaluaciones on-line), y dado que tampoco concurre ninguna otra de las excepciones del artículo 9.2 RGPD, que pueda levantar la prohibición del artículo 9.1 RGPD, procede descartar la existencia de una base jurídica que legitime el tratamiento de datos denunciado.

Dado lo anterior, resultaría innecesario abordar las bases jurídicas invocadas por la entidad previstas en el artículo 6 del RGPD. Sin embargo, se hace a continuación un breve análisis al respecto.

El artículo 6.1 RGPD establece que el tratamiento será lícito si al menos se cumple una de las siguientes condiciones:

- a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;*
- b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado se parte o para la aplicación a petición del mismo de medidas precontractuales;*
- c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento*
- d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;*
- e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;*
- f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un*

niño. Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones”

Como se ha avanzado, la FUOC considera que el sistema del reconocimiento facial es necesario para la ejecución del contrato de prestación de los servicios de educación superior no presencial, suscrito entre la Universidad imputada y el estudiante, de acuerdo con el artículo 6.1 b) RGPD, y argumenta:

La UOC presta un servicio público de educación que se centra en la realización de estudios de calidad no presenciales. La metodología formativa de la UOC está basada al 100% en el canal online, con lo que la evaluación online se convierte en una parte esencial de la relación entre el estudiante y la Universidad (...).

La justificación del contrato es la formalización de la matrícula por parte del estudiante para poder cursar los estudios correspondientes. Por tanto, su esencia radica en posibilitar la prestación de los servicios académicos de educación superior no presenciales requeridos por el estudiante, con las ventajas y rasgos diferenciales que ofrece una Universidad no presencial como la UOC (...).

El contrato de matrícula tiene como elementos esenciales:

- I. La voluntad del estudiante de obtener unos servicios de formación no presencial habiendo elegido formar informada una metodología educativa específica sobre el resto de oferta formativa del mercado*
- II. El consentimiento libre, voluntario e informado que otorga el estudiante al suscribir el contrato mediante la formalización de la correspondiente matrícula; y,*
- III. El objeto del contrato que se suscribe, la prestación de los servicios académicos de educación superior no presencial, de acuerdo con una metodología didáctica propia dirigida a responder a las necesidades educativas de personas que se forman a lo largo de la vida, según lo indicado en las Condiciones Generales de Contratación aceptadas por el estudiante (...)*

El estudiante, cuando se matricula en la UOC, espera recibir un servicio educativo de calidad con las ventajas y flexibilidad de una Universidad no presencial y con todas las garantías de calidad docente que exige la enseñanza universitaria, previniendo, detectando y combatiendo las conductas irregulares derivadas de una educación en esta modalidad, como pueden ser, entre otras, la copia, el plagio o la suplantación de identidad (...) El estudiante tiene derecho a ser evaluado de sus conocimientos y competencias de una forma justa y objetiva, de conformidad con los principios de neutralidad, objetividad, no discriminación e igualdad de oportunidades, de modo que si la UOC no hiciera todo lo posible por evitar el fraude académico en los procesos de verificación de los conocimientos y , permitiera que algunos estudiantes superaran unas pruebas finales de evaluación utilizando medios ilícitos o fraudulentos, estaría frustrando las expectativas académicas de los estudiantes que hacen el esfuerzo de estudiar y esperan que los demás tengan el mismo comportamiento, y podría incurrir en un incumplimiento de contrato.”

Asimismo, la FUOC también sostiene que los y las estudiantes que deciden cursar los estudios en esta Universidad son conocedores de que la educación que imparte la Universidad es en modalidad docente virtual, y no presencial, “utilizando herramientas de verificación de *identidad en los casos de evaluación mediante pruebas de evaluación*

finales". Y añade que, antes de formalizar el contrato con el futuro estudiante, se ofrece información relativa a las condiciones de prestación del servicio académico de carácter docente, entre las que se incluye la relativa a la verificación, tanto de los conocimientos como de la identidad, y que, por tanto, el estudiante " (...) tiene la opción de rechazar este tratamiento de los datos - necesario para la ejecución del contrato con la FUOC -, matriculándose en otro centro docente" .

De acuerdo con lo anterior, la entidad imputada concluye que los datos identificativos del estudiante constituyen parte esencial del proceso de matriculación y de evaluación, a fin de asegurar que el individuo que se está examinando es la misma persona que la que se matriculó por aquellos estudios concretos. Y sobre el consentimiento del estudiante, aduce que *" hay que entender que la suscripción de un contrato, con las características del proceso de matrícula de la UOC, lleva implícito un consentimiento expreso e informado del uso de la tecnología de reconocimiento facial por parte de los estudiantes, ya que se incluye en el concurso de la oferta, como exige el artículo 1262 del Código Civil (...).*

Pues bien, esta Autoridad no cuestiona que el reconocimiento facial pueda ser una herramienta idónea para asegurar que el individuo que se examina es la misma persona que la que se matriculó por estudios concretos. Sin embargo, a efectos de valorar si la adopción de la medida es proporcional, teniendo en cuenta el objeto del contrato celebrado con el estudiante, no está de más señalar que, la STC 207/1993 disponía que, para comprobar si una medida es restrictiva de un derecho fundamental, debe superar el juicio de proporcional, definido en los siguientes términos: *" es necesario constatar si cumple los tres siguientes requisitos o condiciones: «si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad), si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad);y, finalmente, si la misma es ponderada o equilibrada, puede derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)"*.

De acuerdo con ello, cabe afirmar que, si bien el sistema de reconocimiento facial puede ser una herramienta eficaz para controlar y prevenir el fraude académico, lo cierto es que este sistema no cumple con el principio de licitud del tratamiento que impone la normativa de protección de datos, y que existen otras medidas lícitas menos intrusivas e igualmente idóneas para la prevención del fraude académico, puesto que, de acuerdo con las afirmaciones de la FUOC, de los 75.024 estudiantes matriculados en el primer semestre del curso académico 2021-2022 , sólo 31.501 se sometieron a la herramienta del reconocimiento facial - antecedente 5º-, y el sistema de reconocimiento facial se empezó a emplear en fecha 08/01/2022.

En esta línea, el Dictamen 6/2014, del Grupo 29, argumenta que, para valorar la "necesidad" del tratamiento, es necesario tener en consideración si se dispone de otros medios menos invasivos que sirvan para la misma finalidad, así cómo determinar si el contrato se puede ejecutar sin este concreto tratamiento (Dictamen 6/2014 del Grupo 29). Y, tal y como se ha visto, en el presente caso, la entidad imputada podía utilizar otros medios para evaluar al alumnado, como venía haciendo hasta que puso en marcha la herramienta del reconocimiento facial.

Además, dado que la implementación de la tecnología de reconocimiento facial se enmarca en un contexto caracterizado por la ausencia de una norma con rango de ley que establezca los requisitos de licitud de este tipo de tratamiento, no es plausible afirmar la medida adoptada por la FUOC – el uso del sistema del reconocimiento facial – supere el juicio de proporcionalidad, en el sentido de que de su implementación se derivan más beneficios que perjuicios para el interés general.

La FUOC invoca también, como base legitimadora de la realización de pruebas de evaluación final mediante un sistema de reconocimiento facial, el interés legítimo de la Universidad de prevenir la suplantación de identidad y el fraude de los estudiantes en el proceso de evaluación -en línea con el considerante 47 del RGPD-, así como el interés legítimo de todos los estudiantes de ser evaluados en igualdad de condiciones, previniendo el fraude académico.

El artículo 6.1 f) del RGPD determina que el tratamiento será lícito si éste es *necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño. Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones*”.

En relación con este precepto, el considerante 47 del RGPD establece: “ *El interés legítimo de un responsable del tratamiento, incluso el de un responsable al que se puedan comunicar datos personales, o de un tercero, puede constituir una base jurídica para el tratamiento, siempre que no prevalezcan los intereses o derechos y libertades del interesado, teniendo en cuenta las expectativas razonables de los interesados basadas en su relación con el responsable. Tal interés legítimo podría darse, por ejemplo, cuando existe una relación pertinente y apropiada entre el interesado y el responsable, como en situaciones en las que el interesado es cliente o está al servicio del responsable. En cualquier caso, la existencia de un interés legítimo requeriría una evaluación meticulosa, incluso si un interesado puede prever de forma razonable, en el momento y en el contexto de la recogida de datos personales, que pueda producirse el tratamiento a tal fin. En particular, los intereses y derechos fundamentales del interesado podrían prevalecer sobre los intereses del responsable del tratamiento cuando se proceda al tratamiento de las datos personales en circunstancias en las que el interesado no espere razonablemente a que se realice un tratamiento ulterior. Dado que corresponde al legislador establecer por ley la base jurídica para el tratamiento de datos personales por parte de las autoridades públicas, esta base jurídica no debe aplicarse al tratamiento efectuado por las autoridades públicas en el ejercicio de sus funciones. El tratamiento de datos de carácter personal estrictamente necesario para la prevención del fraude constituye también un interés legítimo del responsable del tratamiento de que se trate. El tratamiento de datos personales con fines de mercadotecnia directa puede considerarse realizado por interés legítimo.*”

Al respecto, el Dictamen 06/14, del Grupo del artículo 29, recoge varios elementos que pueden tenerse en consideración para realizar la ponderación que requiere el artículo 6.1 f) RGPD. Entre otros, el referido dictamen alude a la naturaleza de los datos, y al impacto que el tratamiento puede tener sobre los derechos de las personas interesadas. Y, como se ha dicho, cabe concluir que, dada la naturaleza de los datos, la intromisión en la vida privada,

así como la afectación al derecho a la protección de datos del alumnado que debe registrarse en herramienta del reconocimiento facial, procede descartar la concurrencia de la base legitimadora del artículo 6.1.f) RGPD.

Por otra parte, evidenciar que el Considerante 47 RGPD prevé que el tratamiento de datos de carácter personal debe ser " *estrictamente necesario* " para la prevención del fraude, a los efectos de constituir un interés legítimo del responsable del tratamiento. Sin embargo, como ya se ha argumentado, difícilmente puede sostenerse que el reconocimiento facial es estrictamente necesario para controlar la suplantación de identidad del alumnado, cuando existen otras fórmulas que conducen al mismo resultado.

2.2. Alternativa al tratamiento de datos biométricos para la verificación de la identidad del alumnado

En la propuesta de resolución la instructora proponía instar a la FUOC para que " *adopte medidas que aseguren que los y las estudiantes que deben realizar estas pruebas de evaluación puedan optar libre y voluntariamente entre realizar las pruebas por medio de la herramienta del reconocimiento facial, o mediante cualquier otro sistema alternativo que no les resulte especialmente gravoso y que respete la legislación vigente en materia de protección de datos. En este sentido, a efectos de considerar que los y las estudiantes han prestado su consentimiento explícito para someterse a la herramienta del reconocimiento facial, se les deberá informar de manera clara que la elección del sistema de evaluación no comportará ninguna discriminación ni incidirá en modo alguno en su evaluación*".

Pues bien, en relación con este punto, la FUOC en su escrito de alegaciones a la propuesta de resolución, sugiere dos alternativas a efectos de corregir la infracción, que serán analizadas en el fundamento de derecho 5º de esta resolución.

2.3. En relación con la presunta carencia de perjuicios a las personas interesadas

La entidad imputada reitera los argumentos recogidos en los escritos presentados previamente ante la Autoridad , cuando sostiene que el uso del sistema de reconocimiento facial no ha producido ningún perjuicio a los estudiantes matriculados en los estudios que requerían este sistema de evaluación ya que, en todo momento, el alumnado es consciente del uso que la Universidad hará de sus datos personales. Igualmente, manifiesta que se trata de un tratamiento "*transparente, informado y documentado*" y que se ofrece a los estudiantes la posibilidad de ejercer cualquiera de los derechos previstos en la normativa de protección de datos personales, así como de contactar con la delegada de protección de datos personales.

En relación con lo anterior, esta Autoridad no comparte los argumentos de la entidad imputada puesto que no se puede afirmar de forma fehaciente la falta de perjuicios a los y las estudiantes a quienes se ha sometido a un sistema de reconocimiento facial. Al respecto, cabe tener presente que algunos estudiantes han denunciado ante esta Autoridad el tratamiento controvertido, así como el hecho de que la FUOC no ofrece la posibilidad de evaluar al alumnado mediante un sistema alternativo al reconocimiento facial, que sea conforme al RGPD y al LOPDDDD. Y, en relación con lo anterior, cabe añadir la consecuencia de no consentir el referido tratamiento, que se ha asociado a la obtención de la calificación de "No presentado".

En cualquier caso, cabe señalar que, la existencia o la falta de perjuicios no es un elemento exigido por el tipo infractor aplicado, por considerar cometida la infracción.

2.4. En relación con la presunta ausencia de culpabilidad

La entidad imputada pone de manifiesto la carencia de intencionalidad y de culpabilidad, en relación con los hechos que son objeto de este procedimiento. Asimismo, en relación con el principio de culpabilidad, invoca la sentencia número 76/1990, de 26 de abril, del Tribunal Constitucional, de acuerdo con la cual, los principios y garantías presentes en el ámbito del Derecho Penal son aplicables, con ciertos matices, en el ejercicio de cualquier potestad sancionadora de la Administración Pública.

Asimismo, la FUOC también cita la sentencia de 10 de febrero de 1986 del Tribunal Supremo que establece lo siguiente:

“el ejercicio de la potestad punitiva, en cualquiera de sus manifestaciones, debe acomodarse a los principios y preceptos constitucionales que presiden el ordenamiento jurídico penal en su conjunto, y, sea cual sea, el ámbito en el que se mueva la potestad punitiva del Estado, la Jurisdicción, o el campo en que se produzca, viene sujeta a unos mismos principios cuyo respeto legitima la imposición de las penas y sanciones, por lo que, las infracciones administrativas, para ser susceptibles de sanción o pena, deben ser típicas, es decir, previstas como tales por norma jurídica anterior, antijurídicas, esto es, lesivas de un bien jurídico previsto por el Ordenamiento, y culpable, atribuible a un autor a título de dolo o culpa, para asegurar en su valoración el equilibrio entre el interés público y la garantía de las personas que es lo que constituye la clave del Estado de Derecho”.

En último término, en su escrito de alegaciones a la propuesta de resolución, la FUOC concluye que, *considerando que el tratamiento de datos objeto de este procedimiento ha sido ajustado a Derecho, fundamentado en bases de legitimación no discutidas por esta Autoridad y habiendo incorporado propuestas de mecanismos de verificación de identidad alternativos a los interesados que no deseen ser objeto de dicho tratamiento, procede estimar la ausencia total de culpabilidad”.*

Al respecto, en primer lugar, cabe poner de manifiesto que, en contra de lo que argumenta la FUOC, esta Autoridad sí ha discrepado sobre las bases jurídicas invocadas por la entidad y que, a su juicio, legitimaban el tratamiento de los datos biométricos (apartado 2 del fundamento de derecho 2º de esta resolución).

Por otra parte, la concurrencia del elemento culpabilístico, es decir, la necesidad de que exista dolo o culpa en la acción punitiva, es plenamente aplicable al derecho administrativo sancionador, de acuerdo con lo que prevé el artículo 28 de la Ley 40/2015, de 1 de octubre, de régimen jurídico del sector público. Esta necesidad de culpa como elemento constitutivo de la infracción administrativa, ha sido expresamente reconocida por el Tribunal Constitucional, en la sentencia 76/1990, invocada por la FUOC.

Dicho esto, cabe afirmar que, la implantación de un sistema de reconocimiento facial, a efectos de evaluar los conocimientos de los estudiantes, no es una conducta que obedezca a un descuido involuntario sino que la FUOC llevó a cabo el controvertido tratamiento de

forma deseada y conscientemente. En consecuencia, el hecho de que actuara con el convencimiento de que se ajustaba a las previsiones de la normativa de protección de datos vigente, no tiene encaje en un supuesto de carencia de culpabilidad, que permita exonerarla de responsabilidad.

3. En relación con los hechos descritos en el apartado de hechos probados, relativos al uso del sistema de reconocimiento facial para la realización de pruebas de evaluación final, se debe acudir al artículo 5.1 a) del RGPD, que prevé que los datos personales serán “*tratados de manera lícita, leal y transparente en relación con el interesado (“licitud, lealtad y transparencia”)*).

En este sentido, el RGPD dispone que todo tratamiento de datos personales debe ser lícito (artículo 5.1 a) y, a este respecto, establece un sistema de legitimación del tratamiento de datos que se fundamenta en la necesidad de que concurra alguna de las bases jurídicas establecidas en su artículo 6.1, transcrito con anterioridad.

Por su parte, el artículo 9.1 del RGPD, también transcrito, dispone la prohibición de tratar categorías especiales de datos personales (entre ellas, los datos biométricos dirigidos a identificar de forma unívoca a una persona física), no concurrente en el caso presente ninguna de las excepciones previstas en el apartado 2 de dicho precepto, que levantaría tal prohibición.

Durante la tramitación de este procedimiento se ha acreditado debidamente el hecho descrito en el apartado de hechos probados, que es constitutivo de la infracción prevista en el artículo 83.5.a) del RGPD, que tipifica la vulneración de “*los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9*”, entre los que se encuentra el principio de licitud (artículo 5.1 a) en relación con el artículo 9 RGPD.

La conducta que aquí se aborda se ha recogido como infracción muy grave en el artículo 72.1.e) de la LOPDDDD, en la siguiente forma:

“e) El tratamiento de datos personales de las categorías a que se refiere el artículo 9 del Reglamento (UE) 2016/679, sin que se dé alguna de las circunstancias previstas en el citado precepto y el artículo 9 de esta ley orgánica”

4. Al no albergarse la FUOC en ninguno de los sujetos previstos en el artículo 77.1 del LOPDDDD, resulta de aplicación el régimen sancionador general previsto en el artículo 83 del RGPD.

El artículo 83.5 del RGPD prevé para las infracciones allí previstas, se sancionen con una multa administrativa de 20.000.000 de euros como máximo, o tratándose de una empresa, de una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.

Dicho esto, corresponde determinar la cuantía de la multa administrativa que procede imponer. Según lo que establece el artículo 83.2 del RGPD, y también de conformidad con el principio de proporcionalidad consagrado al artículo 29 de la Ley 40/2015, tal y como

indicaba la persona instructora en la propuesta de resolución, procede imponer la sanción de 20.000 euros (veinte mil euros). Esta cuantificación de la multa se basa en la ponderación entre los criterios agravantes y atenuantes que a continuación se indican.

Como criterios atenuantes, se observa la concurrencia de las siguientes causas:

- La realización de una evaluación de impacto por parte de la FUOC en relación con los tratamientos controvertidos (83.2.k RGPD)
- La falta de beneficios obtenidos como consecuencia de la infracción (art. 83.2.k RGPD y art. 76.2.c LOPDGDD)

Por el contrario, como criterios agravantes, hay que tener en cuenta los siguientes elementos :

- La naturaleza, gravedad y duración de la infracción, así como el número de personas afectadas (art. 83.2 a RGPD). De los hechos imputados se desprende que, como mínimo, en fecha 04/11/2022, 31.501 estudiantes han sido sometidos al sistema de reconocimiento facial para ser evaluados, y que los datos que se han recogido de estas personas entran dentro de la calificación de categorías especiales, de acuerdo con el artículo 9.1 RGPD.
- La vinculación de la actividad del infractor con la práctica de tratamientos de datos personales (art. 83.2 b RGPD). En la medida en que la entidad imputada es una Universidad, cabe afirmar que existe una estrecha vinculación entre su actividad educativa y el tratamiento de un número considerable de datos personales – no sólo de estudiantes de grado o posgrados, sino que también investigadores e investigadoras, y otro personal que pueda prestar sus servicios a la entidad -.
- Las categorías de datos de carácter personal afectadas por la infracción (art. 83.2 g RGPD)
- Las sanciones impuestas por esta Autoridad a la entidad imputada por la infracción de la legislación en materia de protección de datos, anterior a los hechos imputados (art. 83.2 e RGPD) - procedimientos sancionadores núm. PS 40/2014, PS 29/2017, y PS 27/2021.
- El carácter continuado de la infracción (art. 76.2 b LOPDGDD)

Por último, cabe señalar que la entidad imputada, en su escrito de alegaciones a la propuesta de resolución, pide la reducción de la cantidad de la multa propuesta por la instructora del procedimiento. En términos literales, la entidad imputada manifiesta lo siguiente:

“Que, en caso de que esta Autoridad considere que debe sancionar a la FUOC, tome en consideración las medidas propuestas, aplicando la sanción en la primera mitad de la parte inferior”.

Sin embargo, ni el RGPD, ni el LOPDGDD, contemplan como atenuante el hecho de que, en el marco de un procedimiento sancionador, la entidad imputada proponga la adopción de determinadas medidas correctoras para evitar que se siga vulnerando la normativa de protección de datos, de hecho, la obligación de todo responsable del tratamiento es evitar vulnerar dicha normativa. El cumplimiento de una obligación no puede, por tanto, considerarse un atenuante, por lo que procede descartar la aplicación de la reducción solicitada por la FUOC.

5. Ante la constatación de las infracciones previstas en el art. 83 del RGPD en relación con ficheros o tratamientos de titularidad privada, el artículo 21.3 de la Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos, faculta a la directora de la Autoridad para que la resolución que declara la infracción establezca las medidas oportunas para que cesen o se corrijan sus efectos.

La persona instructora de este procedimiento proponía requerir a la FUOC para que adoptara medidas que aseguren que el alumnado pueda optar libre y voluntariamente entre realizar las pruebas por medio de la herramienta del reconocimiento facial, o por medio de cualquier otro sistema alternativo que no les resulte especialmente gravoso y que respete la normativa vigente en materia de protección de datos. Así pues, a efectos de considerar que el alumnado ha prestado su consentimiento explícito para someterse a la herramienta del reconocimiento facial, la propuesta de resolución argumentaba que la FUOC debía informar de forma clara que la elección del sistema de evaluación no comportará ninguna discriminación ni incidirá en modo alguno en su evaluación.

Al respecto, la entidad imputada, en las alegaciones a la propuesta de resolución, sugiere, además de facilitar al alumnado la información precontractual que consta tanto en las condiciones generales de contratación, como en la normativa académica y en la política de privacidad, *“ reforzar aún más esta información precontractual mediante la incorporación en el proceso de formalización de la matrícula de un aviso específico relativo al tratamiento de datos biométricos con el fin de verificar la identidad de los estudiantes durante el proceso de evaluación final como elemento necesario de la contratación, así como la imposibilidad de continuar con su formalización en caso de desacuerdo. Es decir, un potencial estudiante que esté en desacuerdo con las metodologías utilizadas por la FUOC puede libremente y de forma informada, decidir no matricularse en ella en virtud del ejercicio de su derecho de elección de centro universitario.”*

La FUOC explica que esta alternativa comprende las siguientes actuaciones:

- (i) *“ Reforzar la comunicación previa al proceso de matrícula. Incluir la información relativa a los métodos de identificación que utiliza la FUOC en fase precontractual , incluido material publicitario de los servicios ofrecidos por la Universidad.*
- (ii) *Reforzar la comunicación durante el proceso de matrícula. Incorporación al proceso de formalización de la matrícula de un aviso específico relativo al tratamiento de datos biométricos con el fin de verificar la identidad de los estudiantes durante el proceso de evaluación final como elemento necesario de la contratación.*
A título de ejemplo, el aviso informativo podría tener el siguiente literal:
“Elegir la UOC como universidad para iniciar o continuar tus enseñanzas universitarias y, por tanto, matricularte en esta Universidad, implica que, en las asignaturas en las que haya prueba de evaluación, se utilizarán herramientas de reconocimiento facial con técnicas biométricas para evitar la suplantación de identidad y el fraude académico. En caso de no estar de acuerdo, no será posible continuar con el proceso de matrícula”.
- (iii) *Imposibilidad de continuar con la formalización de la matrícula, en caso de desacuerdo con la utilización por parte de la FUOC de los tratamientos de datos informados”.*

Seguidamente la entidad imputada sugiere, como medida subsidiaria para el caso de que esta Autoridad no considere ajustada a derecho la primera medida propuesta, la creación de un trámite específico para vehicular la posibilidad de que aquellos estudiantes que así lo deseen, puedan optar por un mecanismo alternativo. En este caso, la alternativa propuesta comprendería lo siguiente:

- (i) *Reforzar la comunicación previa al proceso de matrícula. Incluir la información relativa a los métodos de identificación que utiliza la UOC en fase precontractual, incluido material publicitario de los servicios ofrecidos por la Universidad.*
- (ii) *Crear un trámite específico para garantizar que los estudiantes que no deseen que la UOC lleve a cabo el tratamiento de datos biométricos para la verificación de su identidad, accedan a un mecanismo alternativo. Los mecanismos previstos serán, por regla general, la evaluación presencial o evaluación oral síncrona, puesto que son las vías que podrían equiparar las garantías que ofrece la identificación mediante reconocimiento facial. La selección de uno de estos dos mecanismos, o de otro en su caso, será determinado por la Universidad en atención a criterios docentes.*
- (iii) *Reforzar la comunicación posterior al proceso de matrícula, incluir la información relativa al trámite específico que posibilita la alternativa al uso de datos biométricos para aquellos estudiantes que lo deseen.*

Al respecto, cabe señalar que la primera alternativa que plantea la entidad imputada implica condicionar la matriculación, a la aceptación del tratamiento de los datos personales del alumnado, mediante la herramienta del reconocimiento facial. Una propuesta que no se ajusta a la medida que propuesta por la instructora del procedimiento dado que no corrige los efectos de la infracción, ni respeta la normativa de protección de datos, por los motivos que a continuación se esgrimen.

Precisamente los hechos que se imputan en el presente procedimiento son constitutivos de infracción dado que se condiciona la participación en unas pruebas de evaluación, al tratamiento de los datos personales del alumnado, mediante la herramienta del reconocimiento facial, sin que los y las estudiantes dispongan de una alternativa al tratamiento de sus datos biométricos, para realizar las pruebas de evaluación. Así pues, condicionar la matriculación, a la aceptación del tratamiento controvertido, contraviene igualmente la normativa de protección de datos, en la medida en que el alumnado tampoco dispone de un mecanismo alternativo al tratamiento de datos controvertido, a fin de poder cursar los estudios deseados.

La segunda alternativa que plantea la FUOC, como medida correctora de los efectos de la infracción que aquí se imputa, consiste en reforzar la información que se facilita al alumnado antes y después de matricularse, crear un trámite específico para aquellos estudiantes que rechacen someterse a la herramienta del reconocimiento facial, y ofrecerles la opción de ser evaluados de forma presencial o bien mediante “la evaluación oral síncrona”.

Esta segunda propuesta de la FUOC se ajusta a la propuesta por la instructora de este procedimiento, en tanto en cuanto ofrece al alumnado alternativas al sistema de reconocimiento facial para poder ser evaluados, asistencia presencial o bien una evaluación oral síncrona, en el bien entendido que la evaluación oral síncrona no puede comportar el tratamiento de datos biométricos destinados a identificar de forma unívoca a una persona

física, y que el alumnado que rechace someterse al sistema de reconocimiento facial, para que el sistema alternativo no les resulte especialmente gravoso, deben poder escoger entrega entre una de estas dos opciones propuestas por la FUOC. Asimismo, y respecto a los estudiantes que acepten ser evaluados utilizando la herramienta del reconocimiento facial, la FUOC deberá recoger su consentimiento explícito para el tratamiento de sus datos biométricos.

A la vista de lo expuesto, procede requerir a la FUOC para que lo antes posible, y en todo caso en el plazo máximo de 1 mes a contar desde el día siguiente de la notificación de esta resolución, ofrezca a su alumnado una doble alternativa al sistema de reconocimiento facial para realizar las pruebas de evaluación, es decir, que puedan escoger libremente entre un sistema de asistencia presencial o una evaluación oral síncrona que no comporte el tratamiento de datos biométricos, y recogiendo en todo caso el consentimiento explícito de aquellos alumnos que opten por el sistema del reconocimiento facial para su evaluación.

Una vez adoptadas las medidas correctoras descritas en el párrafo anterior en el plazo señalado, en el plazo de los 10 días siguientes la FUOC debe informar a la Autoridad, sin perjuicio de la facultad de inspección de esta Autoridad para efectuar las verificaciones correspondientes.

Por todo esto, resuelvo:

1. Imponer a la Fundación para la Universitat Oberta de Catalunya la sanción consistente en una multa de 20.000.- euros (veinte mil euros), como responsable de una infracción prevista en el artículo 83.5.a) en relación con el artículo 5.1 a) y 9, ambos del RGPD.
2. Requerir a la Fundación para la Universitat Oberta de Catalunya para que adopte las medidas correctoras señaladas en el fundamento de derecho 5º in fine, y acredite ante esta Autoridad las actuaciones llevadas a cabo para cumplirlas.
3. Notificar esta resolución a la Fundación para la Universidad Oberta de Catalunya.
4. Ordenar que se publique esta resolución en la web de la Autoridad (apdcat.gencat.cat), de conformidad con el artículo 17 de la Ley 32/2010, de 1 de octubre.

Contra esta resolución, que pone fin a la vía administrativa de acuerdo con los artículos 26.2 de la Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos, y 14.3 del Decreto 48/2003, de 20 de febrero, por el que se aprueba el Estatuto de la Agencia Catalana de Protección de Datos, la entidad imputada puede interponer, con carácter potestativo, un recurso de reposición ante la directora de la Autoridad Catalana de Protección de Datos, en el plazo de un mes a contar desde el día siguiente de su notificación, de acuerdo con lo que prevén el artículo 123 y siguientes de la LPAC. También puede interponer directamente un recurso contencioso administrativo ante los Juzgados de lo Contencioso-Administrativo, en el plazo de dos meses a contar desde el día siguiente de su notificación, de acuerdo con los artículos 8, 14 y 46 de la Ley 29/1998, de 13 de julio, reguladora de la jurisdicción contencioso-administrativa.

Si la entidad imputada manifiesta a la Autoridad su intención de interponer recurso contencioso administrativo contra la resolución firme en vía administrativa, la resolución se suspenderá cautelarmente en los términos previstos en el artículo 90.3 de la LPAC.

Igualmente, la entidad imputada podrá interponer cualquier otro recurso que estime conveniente para defender sus intereses.

La directora,

Traducción automática