N/REF: 0036/2020

La consulta plantea una serie de cuestiones relativas al uso de técnicas de reconocimiento facial en la realización de pruebas de evaluación online, partiendo de que el estado de alarma declarado por Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19, ha determinado la migración de todas las actividades docentes a entornos online.

Para ello, la consulta parte de que un elemento determinante en la prestación del servicio público de educación superior consiste en la verificación objetiva de los conocimientos de los estudiantes, destacando que "con motivo de la realización de un examen se vienen tratando distintos tipos de datos en el mundo físico. Uno de los tratamientos usuales durante la realización de un examen consiste en la verificación de la identidad de la persona examinada, ya sea a la entrada en el aula, durante la realización de la prueba o al final de la misma a la entrega de la documentación. Para ello se exige la exhibición de un documento identificativo, DNI, tarjeta de residencia, pasaporte, o carné universitario.

Como resulta evidente, la presencia física en el aula del profesorado impide que, por ejemplo, un estudiante pudiera abandonar su sitio siendo suplantado en su identidad por otra persona, o que un estudiante realizara la prueba de evaluación haciéndose pasar por otro. Sin embargo, esta posibilidad de control y vigilancia se desaparece por completo cuando se trata de realizar un examen online desde el propio domicilio del estudiante. En este sentido la identificación debe realizarse:

- Mediante la asignación de identificadores de acceso a entornos de aula virtual.
- Mediante el visionado remoto del estudiante mediante herramientas de videoconferencia o webcams".

No obstante lo anterior, la consulta destaca que "a los medios tradicionales se ha sumado la existencia de herramientas de reconocimiento facial. Estas herramientas en su nivel más preciso deberían poder asegurar la identificación unívoca de la persona examinada e incluso detectar expresiones faciales que identificaran un comportamiento anómalo. En cualquier caso, en su nivel más simple son capaces de establecer un patrón facial de la persona que inicia el examen frente a una pantalla y garantizar que:

- La persona no se ha desplazado o abandonado su sitio frente al terminal durante el periodo asignado a la realización de la prueba.
- No ha sido sustituida por persona distinta."

Atendiendo a la definición de datos biométricos recogida en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD), la consulta se centra en los supuestos que podrían permitir el tratamiento de dichos datos conforme al artículo 9 del RGPD, singularmente el consentimiento o el interés público esencial, así como en las condiciones y garantías adecuadas a las que debería someterse el tratamiento de los datos por parte de las universidades, atendiendo especialmente a la situación derivada de la declaración del estado de alarma, solicitando que el informe se emita con la mayor celeridad posible, puesto que "la realización de los exámenes correspondientes a la evaluación final del curso académico es inminente".

La citada consulta, en la que se solicita su tramitación con "la mayor celeridad posible, puesto que la realización de los exámenes correspondientes a la evaluación final del curso académico es inminente", se ha recibido en la Agencia Española de Protección de Datos el pasado 27 de abril, con posterioridad a los trabajos realizados por la CRUE durante los meses de marzo y abril y que han dado lugar a la publicación del "Informe sobre Procedimientos de Evaluación no Presencial. Estudio del Impacto de su Implantación en las Universidades Españolas y Recomendaciones" de 16 de abril de 2020 y de la "Guía sobre la protección de datos personales en el ámbito universitario en tiempos del COVID-19" del pasado 24 de abril, respecto de los cuales no se ha consultado a esta Agencia, por lo que no ha podido contribuir a dar seguridad jurídica a la comunidad educativa con carácter previo al inicio de la realización de las evaluaciones on line.

I

Antes de entrar a analizar las cuestiones planteadas en la consulta, esta Agencia considera necesario realizar una serie de consideraciones de carácter general en relación con la misma.

En primer lugar, atendiendo a la concreta referencia que en el escrito de consulta se realiza a la situación creada como consecuencia del estado de alarma, debe señalarse que el mismo no implica la suspensión del derecho fundamental a la protección de datos, sin perjuicio de que el mismo pueda verse afectado como consecuencia del hecho causal que ha dado lugar a la declaración, previendo el propio RGPD los cauces adecuados que permiten dar respuesta a la situación de crisis sanitaria respetando el derecho fundamental a la protección de datos personales. En este sentido se ha venido pronunciando reiteradamente esta Agencia desde su Informe 17/2020:

> "Examinada su solicitud de informe, en relación con los tratamientos de datos resultantes de la actual situación derivada de la extensión del virus COVID-19, en primer lugar, con carácter general, debe aclararse que la normativa de protección de datos personales, en tanto que dirigida a salvaguardar un derecho fundamental, se aplica en su integridad a la situación actual, dado que no existe razón alguna que determine la suspensión de derechos fundamentales, ni dicha medida ha sido adoptada.
>
> Sin perjuicio de lo anterior, la propia normativa de protección de datos personales (Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, RGPD) contiene las salvaguardas y reglas necesarias para permitir legítimamente los tratamientos de datos personales en situaciones, como la presente, en que existe una emergencia sanitaria de alcance general. Por ello, al aplicarse dichos preceptos previstos para estos casos en el RGPD, en consonancia con la normativa sectorial aplicable en el ámbito de la salud pública, las consideraciones relacionadas con la protección de datos -dentro de los límites previstos por las leyes- no deberían utilizarse para obstaculizar o limitar la efectividad de las medidas que adopten las autoridades, especialmente las sanitarias, en la lucha contra la epidemia, por cuanto ya la normativa de protección de datos personales contiene una regulación para dichos casos que compatibiliza y pondera los intereses y derechos en liza para el bien común".

Por consiguiente, todo tratamiento de datos personales que deba realizarse como consecuencia de la pandemia y de la declaración del estado de alarma deberá respetar el derecho fundamental a la protección de datos personales, ajustándose a las previsiones del RGPD, el cual permite, como hemos visto, establecer reglas específicas respecto del ejercicio de dicho derecho, ajustado al propio RGPD, así como a la doctrina elaborada por el Tribunal Constitucional al interpretar el artículo 18.4 de nuestra Constitución, singularmente en lo relativo al principio de proporcionalidad, tal y como se analizará posteriormente.

En segundo lugar, debe destacarse que la realización de evaluaciones online no es algo novedoso ni generado por el estado de alarma, sino que se trata de un método de evaluación que viene aplicándose por algunas universidades españolas desde hace años, siendo diferentes los métodos empleados por éstas para verificar la identidad de los alumnos, que es la principal cuestión en la que se centra la consulta. A estos efectos, tal y como se señala en la misma, existen métodos alternativos al reconocimiento facial y que se han venido aplicando hasta la fecha, como la asignación de identificadores de acceso o el empleo de herramientas de videoconferencia o webcams. Y, en relación con el reconocimiento facial, existen proyectos específicos que vienen

trabajando en el mismo desde hace años para su aplicación en el ámbito universitario, incluso con participación de alguna universidad española, como es el proyecto de innovación e investigación TeSLA (Adaptive Trust-based e-assessment System for Learning) de la Unión Europea, liderado por la Universitat Oberta de Catalunya (UOC) y financiado por la Comisión Europea dentro del programa marco europeo Horizon 2020. Por otro lado, la implantación del reconocimiento facial en la evaluación online no está exenta de dificultades, algunas de las cuales exceden al ámbito específico de la protección de datos pero que tienen incidencia en el mismo, como son las derivadas de la falta de equipamiento tecnológico y de competencias digitales en el profesorado y en el alumnado, la necesidad de atender a los estudiantes con necesidades especiales y otro tipo de problemas de carácter técnico o económico.

Precisamente, estas circunstancias han llevado a la propia entidad consultante a organizar un "Foro Online de Experiencias ante la Suspensión de la Actividad Docente Presencial en Universidades Españolas por el COVID-19" en el que se han planteado las dificultades derivadas de la implantación de sistemas de reconocimiento facial, incluidas las relativas a la privacidad, así como la conveniencia de utilizar otro tipo de medidas, tal y como se detallan en el “Resumen de la Segunda Jornada Online para Compartición de Experiencias de Modelos de Evaluación” celebrada el 26 de marzo de 2020 y en la grabación de dicha sesión a la que enlaza el propio documento (https://www.us.es/sites/default/files/comunicacion/coronavirus/resumen-jornada-modelos-evaluacion.pdf). Entre las medidas posibles para evaluación online, se incide en la necesidad de potenciar la evaluación continua mediante prácticas, trabajos y otro tipo de actividades y el uso de herramientas antiplagio, limitando los supuestos en los que sea necesaria una prueba final de conocimientos, en los que igualmente se pueden adoptar otras medidas para acreditar los mismos, evitando las preguntas memorísticas, estableciendo periodos breves para que se proceda a su respuesta, estableciendo una monitorización del alumno por parte del profesorado y personal de asistencia mediante videoconferencia, realización de exámenes orales por videoconferencia, videos explicativos elaborados por los alumnos, etc. En este mismo sentido, la “Guía de recomendaciones para la evaluación online en las Universidades Públicas de Castilla y León”, elaborada por el “Grupo de Responsables de Docencia Online de las Universidades Públicas de Castilla y León”, en su versión de 3 de abril de 2020 (https://www.usal.es/files/2020_04_03_Recomendaciones_evaluacion_online_para_las_Universidades_Publicas_de_Castilla_y_Leon_V0.7.pdf), recomienda con carácter general y siempre que sea posible, la evaluación continua de las asignaturas, y solo en último caso, recurrir a soluciones de reconocimiento facial o e-proctoring, reservando esta opción para las asignaturas complejas con un gran número de estudiantes.

Idéntico criterio es el que sigue la propia CRUE en su “Guía sobre la protección de datos personales en el ámbito universitario en tiempos del

COVID-19" del pasado 24 de abril, (http://www.crue.org/Documentos%20compartidos/Informes%20y%20Posicionamientos/Guia%20Crue%20Universidades%20Espa%C3%B1olas%20-%20Grupo%20DPD-%20FAQS%20COVID19.pdf), en la que se indica lo siguiente.

> Pregunta 11: ¿Cómo se puede identificar al alumnado? ¿Se pueden usar datos biométricos o imágenes? ¿Qué métodos de identificación del alumnado se pueden emplear?
>
> El Estatuto del Estudiante Universitario permite al profesorado solicitar la identificación del alumnado, quien deberá exhibir su carnet de estudiante o documento identificativo (art.25.7). En un entorno online, se puede solicitar igualmente al alumnado que se identifique mostrando dicha documentación.
>
> En todo caso, para la identificación del estudiantado se recomienda utilizar las medidas técnicas de las que ya dispone la propia universidad y que supongan la medida menos intrusiva para su privacidad.
>
> Utilizar mecanismos de reconocimiento que empleen datos biométricos, más allá del uso de la imagen personal, requiere no sólo de la necesaria base legítima, sino de un análisis documentado de los riesgos vinculados al tratamiento de imágenes del que deriven la adopción de garantías específicas sin olvidar, para el caso de estar contratando dichos servicios a un tercero, la necesaria firma del correspondiente acuerdo o compromiso entre la universidad responsable y el tercero encargado (art. 28 RGPD y art. 33 LOPDGDD).
>
> El Grupo de trabajo de la CRUE integrado por DPDs de las universidades españolas considera no recomendable las técnicas de reconocimiento facial. Debido a su complejidad técnica y al alto grado de exigencia que la legislación plantea al uso de datos biométricos, no es posible abordar esta cuestión sino desde la técnica de una evaluación de impacto relativa a la protección de datos. Por otra parte, la indefinición de las normas obliga a un proceso de interpretación de las habilitaciones para su uso que hace recomendable: Obtener un pronunciamiento expreso de las autoridades de protección de datos con competencia en la materia o definir junto con ellas el modelo de cumplimiento; y considerar las condiciones de regulación que ofrezcan una adecuada seguridad jurídica.

Obviamente, no corresponde a esta Agencia definir los medios a través de los cuales debe procederse a la evaluación de los alumnos, función que corresponde a las universidades y que deberán ser acreditados por las correspondientes agencias de evaluación, pero sí velar por que los mismos se

ajusten a lo previsto en la normativa de protección de datos personales, siendo especialmente relevante a la hora de apreciar la proporcionalidad del tratamiento la existencia de otro tipo de medidas que puedan ser menos restrictivas para el derecho fundamental a la protección de datos personales. Y si bien esto se analizará posteriormente en el presente informe, esta Agencia considera necesario realizar una advertencia con carácter general, atendiendo a la urgencia con la que se solicita el presente informe dada la proximidad de los exámenes del presente curso académico: **refiriéndose la consulta al empleo de técnicas de reconocimiento facial que implican una mayor intrusión en el derecho a la protección de datos personales, y existiendo medidas alternativas para la evaluación online planteadas por la propia comunidad universitaria que permiten hacer frente a la situación generada por la declaración del estado de alarma, así como teniendo en cuenta que el Gobierno ya ha iniciado el plan de desescalada que podría permitir realizar, con las restricciones que se establezcan, pruebas presenciales, debe primar un criterio de prudencia que permita un análisis sosegado de sus implicaciones y, en todo caso, y por lo que respecta a las competencias de esta Agencia, un riguroso estudio de los riesgos que implican esos tratamientos y de las garantías necesarias para proteger el derecho a la protección de datos personales, atendiendo al principio de responsabilidad proactiva y la necesidad de realizar los correspondientes análisis de riesgos, evaluaciones de impacto en la protección de datos y, en su caso, consulta previa a la autoridad de control.**

Por último, el presente informe se centrará en el análisis jurídico planteado en la consulta sin entrar a analizar detenidamente el resto de medidas menos intrusivas que pueden adoptarse para realizar las evaluaciones online, las cuales deberán igualmente respetar los principios establecidos en la normativa sobre protección de datos personales. Y teniendo en cuenta la generalidad con la que se plantea la consulta, en la que no se facilitan datos específicos del tratamiento de reconocimiento facial y otros tipos de tratamientos de datos personales que puedan realizarse, la respuesta a la misma solo puede realizarse con la misma generalidad.

II

Como hemos visto, la consulta se refiere a la utilización de técnicas de reconocimiento facial de los alumnos con el fin de acreditar su identidad en los procesos de evaluación online, partiendo de lo dispuesto en el artículo 46.3 de la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, que establece que “las Universidades establecerán los procedimientos de verificación de los conocimientos de los estudiantes”, precepto que debe completarse, a los efectos de este informe, con lo previsto en el Real Decreto 1791/2010, de 30 de diciembre, por el que se aprueba el Estatuto del Estudiante Universitario, cuyo artículo 25.7 dispone que “En cualquier momento de las pruebas de evaluación,

el profesor podrá requerir la identificación de los estudiantes asistentes, que deberán acreditarla mediante la exhibición de su carné de estudiante, documento nacional de identidad, pasaporte o, en su defecto, acreditación suficiente a juicio del evaluador".

Esta Agencia ya ha tenido ocasión de pronunciarse en relación con los tratamientos de datos personales derivados de la necesaria evaluación de los alumnos, entendiendo, con carácter general, que los mismos se encontrarían amparados por el artículo 6.1.e) del RGPD, como consecuencia de la existencia de un interés público derivado de la configuración de la educación superior como un servicio público por la LOU, si bien deben respetarse en todo caso los principios relativos a la protección de datos recogidos en el artículo 5 del RGPD, correspondiendo a cada universidad, en virtud de su autonomía y del principio de responsabilidad proactiva, velar por el adecuado cumplimiento de los mismos.

En este sentido, se pronunciaba nuestro informe 30/2019, posteriormente reiterado en el informe 63/2019 solicitado por la consultante, al analizar la base jurídica que legitimaría la publicación de las calificaciones de los alumnos:

> En el momento de la emisión del presente informe deberá estarse a lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, RGPD), plenamente aplicable desde el 25 de mayo de 2018 y a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).
>
> El citado Reglamento extiende su protección, tal y como establece su artículo 1.2, a los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales, definidos en su artículo 4.1 como "toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona."

Asimismo, el artículo 4.1 define “tratamiento” como “cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción”.

Por lo tanto, la publicación de las calificaciones de los alumnos, en la medida que contiene datos personales relativos a personas físicas, queda sometida a lo dispuesto en el RGPD.

Por otro lado, es preciso recordar, como ya se ha indicado en reiteradas ocasiones por esta Agencia que la reforma operada por el Reglamento general de protección de datos respecto del régimen contenido en la Ley Orgánica 15/1999 exige un cambio de perspectiva en lo que respecta a los principios articuladores del derecho fundamental a la protección de datos de carácter personal y, en particular, a aquél que hacía del “principio de consentimiento” el eje central del derecho a la protección de datos.

En efecto, si bien la Ley Orgánica y el Reglamento no difieren excesivamente en lo que atañe a la enumeración de las causas legitimadoras del tratamiento, se produce una modificación sumamente relevante en el modo en que dichas causas aparecen recogidas por los textos aplicables: así, mientras del tenor de la Ley Orgánica 15/1999 parecía deducirse que la regla básica de legitimación era, con carácter general, el consentimiento, resultando las restantes causas legitimadoras excepcionales en relación con el consentimiento, que como regla general debía regir el tratamiento, en el texto del artículo 6.1 del Reglamento general de protección de datos el consentimiento se recoge como una de las seis causas de legitimación para el tratamiento sin ostentar mayor o menor importancia que las restantes que en a norma se enumeran.

A mayor abundamiento, el propio Reglamento general de protección de datos pone de manifiesto que el consentimiento del afectado no debe constituir la base legal del tratamiento en determinados supuestos. Así,

el considerando 42 señala en su última frase que “El consentimiento no debe considerarse libremente prestado cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno” y el considerando 43 añade que “Para garantizar que el consentimiento se haya dado libremente, este no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibro claro entre el interesado y el responsable del tratamiento, en particular cuando dicho responsable sea una autoridad pública y sea por lo tanto improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular”.

De este modo, no procede recabar en ningún caso el consentimiento del afectado en los supuestos en los que el tratamiento se encuentre amparado por cualquiera de las causas incluidas en las letras b) a f) del artículo 6.1 del Reglamento general de protección de datos; es decir cuando:

b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este 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 los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

En el presente caso, el artículo 1.1 de la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades califica a la educación superior como un servicio público, señalando que “la Universidad realiza el servicio público de la educación superior mediante la investigación, la docencia y el estudio”, calificación que se reitera en los artículos 27 bis 1.b) y 31.1.a). En virtud de la autonomía universitaria, corresponde a las Universidades la “verificación de los conocimientos de los estudiantes” (artículo 2.2.f) reiterando el artículo 46.3 que “las Universidades establecerán los procedimientos de verificación de los conocimientos de los estudiantes”.

Por consiguiente, como señalaba el informe 178/2014, el legislador ha reconocido la existencia de un interés público, por lo que la publicación de las calificaciones universitarias encontraría su base jurídica en los previsto en el artículo 6.1.e) del RGPD (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) derivada de una competencia atribuida por una norma con rango de ley conforme al artículo 8.2 de la LOPDGDD.

Por otro lado, aun no tratándose los procedimientos de evaluación de procedimientos de concurrencia competitiva, las calificaciones obtenidas van a tener incidencia, tal y como se plantea en la consulta, en el otorgamiento de las matrículas de honor limitadas a un número de estudiantes, así como también en la concesión de premios extraordinarios, por lo que también podría apreciarse un interés legítimo de los alumnos del grupo en el conocimiento de las calificaciones de sus compañeros, al amparo de lo previsto en la letra f) del artículo 6.1. del RGPD.

II

Por lo tanto, siendo lícita la publicación de las notas obtenidas conforme a lo indicado en el apartado anterior, deberá respetarse en todo caso los principios recogidas en el artículo 5 del RGPD, especialmente los de limitación de la finalidad, minimización de datos, limitación del plazo de conservación, integridad y confidencialidad, realizando la publicación de modo que suponga la menor injerencia en los derechos y libertades de los interesados, lo que excluye la posibilidad

de un conocimiento generalizado de las calificaciones, como podría ocurrir en el caso de que se procediera a su publicación en internet, en el que el riesgo se incrementaría además como consecuencia de la posible indexación por los motores de búsqueda.

Por ello se considera como medio preferente para proceder a dicha publicación, que la misma se realice en una intranet o aula virtual en la que estuviera limitado el acceso a los profesores y compañeros del grupo. En el caso de que no fuera posible, podrá realizarse en los tablones de anuncios del centro, siempre que no se encuentren en las zonas comunes de los centros, se garantice que el acceso a los mismos queda restringido a dichas personas y se adopten las medidas necesarias para evitar su público conocimiento por quienes carecen de interés en el mismo.

En cuanto a los datos a publicar, atendiendo al principio de minimización, deberán limitarse al nombre y apellidos del alumno y la calificación obtenida. Solo en el caso de que hubiera alumnos con los mismos nombres y apellidos, deberá publicarse para ellos el número del DNI, aplicando lo previsto en el apartado 1 párrafo primero de la disposición adicional séptima de la LOPDGDD. Por lo tanto, solo en el caso de coincidencia del nombre y apellidos, se publicarán cuatro cifras aleatorias de su documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente, recomendándose por esta Agencia que se sigan los criterios contenidos en el documento “Orientación para la aplicación provisional de la disposición adicional séptima de la LOPDGDD”, disponible en www.aepd.es.

Y en cuanto al tiempo en el que deberá mantenerse dicha publicación, los datos deberán ser “mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales” (artículo 5.1.e). Por tanto, en el caso de las calificaciones provisionales, tal y como se refiere en la consulta, mientras transcurre el plazo para presentar reclamaciones, y las calificaciones definitivas durante el tiempo imprescindible que garantice su conocimiento por todos los interesados.

En todo caso, en virtud de la autonomía universitaria reconocida en el artículo 27 de la Constitución Española y en la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, y ostentando la Universidad consultante la condición de responsable del tratamiento conforme al RGPD, a la misma corresponderá apreciar la necesidad de proceder a la publicación de las calificaciones y la forma en la que deberá realizarse la misma, atendiendo a los criterios señalados en el presente informe y al principio de responsabilidad proactiva en el que se fundamenta la vigente normativa en materia de protección de datos personales.

En este mismo sentido, el mismo informe 63/2019 consideraba amparado por el artículo 6.1.e) la grabación de los exámenes orales o de la sesión docente por el profesor:

Se plantea a continuación si la grabación de exámenes orales y de las sesiones de docencia puede fundamentarse igualmente en el artículo 6.1.e) del RGPD.

En este punto, el artículo 46.3 de la LOU prevé que “Las Universidades establecerán los procedimientos de verificación de los conocimientos de los estudiantes”. Asimismo, en su apartado 2 el citado precepto reconoce a los estudiantes el derecho a “la publicidad de las normas de las Universidades que deben regular la verificación de los conocimientos de los estudiantes” y a “la garantía de sus derechos, mediante procedimientos adecuados y, en su caso, la actuación del Defensor Universitario”, siendo los Estatutos y las normas de organización y funcionamiento las que desarrollarán los derechos y los deberes de los estudiantes, así como los mecanismos para su garantía.

Son, por tanto, los Estatutos y las normas de organización y funcionamiento los que regulan los procedimientos de revisión de las evaluaciones de los alumnos, lo que incluye en ocasiones su revisión ante órganos colegiados (Tribunal de Reclamaciones, Comisión de Revisión u otras denominaciones), así como se establecen plazos de conservación de los exámenes a fin de que los estudiantes puedan presentar las reclamaciones oportunas.

Por consiguiente, la grabación de los exámenes orales puede ser necesaria como medio de prueba para el ejercicio de sus derechos por parte del alumno, así como para que el profesor pueda justificar la evaluación realizada, sin perjuicio de que puedan admitirse otros medios probatorios (por ejemplo, exigir al alumno un esquema de lo que va a exponer).

Por consiguiente, con la finalidad señalada, y siempre que las normas internas de la Universidad prevean la grabación de los exámenes orales, el tratamiento se encontrará fundamentado en lo previsto en el artículo 6.1.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.

En cuanto a la grabación de las sesiones docentes, hay que diferenciar, tal y como hace la consulta, en función de que la grabación se lleve a cabo por el propio docente, la cual puede ser conveniente o incluso necesaria (por ejemplo, en universidades a distancia) para el ejercicio de la función educativa, cuyo fundamento se encontraría igualmente en el artículo 6.1.e), debiendo limitarse su acceso al personal docente y a los alumnos a los que vaya dirigida, sin que pueda ser utilizada ulteriormente para otros fines, como su divulgación pública, que requeriría del consentimiento expreso de los afectados.

Por otro lado, en el caso de que la grabación se realice por la propia Universidad con fines de control laboral, su fundamento se encontraría en el artículo 6.1.b): el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales, siendo de aplicación lo dispuesto en el artículo 89 de la Ley Orgánica 3/2018.

En cuanto a la grabación de la sesión por los alumnos presentes en la sesión docente, debería identificarse la finalidad concreta de dicha grabación, que requerirá, en todo caso, del consentimiento del docente, así como del resto de los alumnos si su imagen o su voz pudieran ser objeto de grabación.

Por el contrario, el informe 186/2017 referido a la posible instalación de videocámaras para la grabación de las imágenes de los alumnos durante la realización de los exámenes en el entorno de una Universidad, con la finalidad de disuadir o, en su caso, acreditar, actuaciones fraudulentas durante los exámenes, consideró desproporcionada la misma. Y si bien dicho criterio se fundamentaba en la normativa anterior, sus consideraciones sobre la proporcionalidad son plenamente aplicables en el momento actual:

> En relación con la instalación de sistemas de videocámaras, la Instrucción 1/2006 hace especial referencia a la necesidad de ponderar los bienes jurídicos protegidos. Así viene a señalar expresamente que, la instalación de este tipo de dispositivos se deberá respetar el principio de proporcionalidad, valorando así la posibilidad de adoptar otros medios menos intrusivos a la intimidad de las personas, con el fin de prevenir interferencias injustificadas en los derechos y libertades fundamentales. (…)
>
> En cuanto a la proporcionalidad, tal y como señala la propia Instrucción, la Sentencia del Tribunal 207/1996 determina que se trata de *"una exigencia común y constante para la constitucionalidad de cualquier medida restrictiva de derechos fundamentales, entre ellas las que supongan una injerencia en los derechos a la integridad física y a la intimidad, y más en particular de las medidas restrictivas de derechos fundamentales adoptadas en el curso de un proceso penal viene determinada por la estricta observancia del principio de proporcionalidad.*
>
> *En este sentido, hemos destacado que, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, 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, por 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)*".
>
> Por consiguiente, cualquier medida de control que se adopte debe superar este juicio de proporcionalidad, determinando si la medida es adecuada, necesaria y equilibrada, ya que en otro caso resulta desproporcionada y por ello contraria a la normativa de protección de datos

Esta Agencia ha venido señalando que cuando se pretendan instalar sistemas de videovigilancia, deberán ponderarse los derechos y garantizarse el cumplimiento estricto del principio de proporcionalidad, debiendo en todo caso respetarse el derecho a la intimidad, a la propia imagen y a la protección de datos.

Así, el artículo 4 de la Instrucción 1/2006 recoge los principios de calidad, proporcionalidad y finalidad del tratamiento estableciendo lo siguiente:

"1.- De conformidad con el artículo 4 de la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal, las imágenes sólo serán tratadas cuando sean adecuadas, pertinentes y no excesivas en relación con el ámbito y las finalidades determinadas, legítimas y explícitas, que hayan justificado la instalación de las cámaras o videocámaras.

2.- Sólo se considerará admisible la instalación de cámaras o videocámaras cuando la finalidad de vigilancia no pueda obtenerse mediante otros medios que, sin exigir esfuerzos desproporcionados, resulten menos intrusivos para la intimidad de las personas y para su derecho a la protección de datos de carácter personal.

3.- Las cámaras y videocámaras instaladas en espacios privados no podrán obtener imágenes de espacios públicos salvo que resulte imprescindible para la finalidad de vigilancia que se pretende, o resulte imposible evitarlo por razón de la ubicación de aquéllas. En todo caso deberá evitarse cualquier tratamiento de datos innecesario para la finalidad perseguida." (…)

Atendiendo a lo que acabamos de indicar y en relación con la cuestión que se plantea en la consulta:

La instalación de cámaras de videovigilancia sería una medida proporcional y justificada si se cumplen los siguientes requisitos:

1. Que se trate de una medida susceptible de conseguir el objetivo propuesto.
2. Que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia.
3. Que la misma sea ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto".

Considerando los criterios de ponderación antes citados, difícilmente puede entenderse que la medida propuesta de grabar a través de sistemas de videovigilancia el interior de las aulas cuando se celebren exámenes, e implementarla con carácter general en una Universidad, sea proporcionada y adecuada para la finalidad perseguida. Tampoco consideramos que la misma constituya un acto necesario para realizar un adecuado seguimiento de la evaluación de los alumnos en los términos señalados por la consulta, pudiendo valorarse otros medios menos intrusivos para la intimidad de las personas, retomando las palabras del art. 4 de la Instrucción antes citado.

En este sentido, sin un bien jurídico superior que lo justifique o si se puede disponer de medios alternativos menos intrusivos para la privacidad de los alumnos, puede resultar desproporcionada la instalación de cámaras en las aulas con la finalidad de videovigilancia y sólo podría considerarse bajo determinadas circunstancias y con especiales salvaguardas, pero no como una medida a implementar con carácter general en la Universidad. En primer lugar, recordemos que se está planteando la captación de imágenes en el interior de un espacio semi privado, en sentido técnico jurídico (entre otras muchas resoluciones, así lo indica el Auto del Tribunal Supremo (Sala de lo Civil, Sección 1ª) de 14 abril 2009), y al menos en lo que a las aulas se refiere. La actuación pretendida pudiera constituir una intromisión ilegítima en los términos previstos en la Ley Orgánica 1/1982 de 5 de mayo de protección civil, cuestión a valorar por los tribunales civiles y no directamente por esta Agencia.

Otra cosa sería que su necesidad se justificara por razones concretas. Para justificar la instalación de una cámara es necesario un motivo objetivo.

Así, en relación con los derechos fundamentales, el art. 52.1 *in fine* de la Carta de los Derechos Fundamentales de la UE, señala que" cualquier limitación del ejercicio de los derechos y libertades reconocidos por la presente Carta deberá ser establecida por la ley y respetar el contenido esencial de dichos derechos y libertades. Dentro del respeto del principio de proporcionalidad, sólo podrán introducirse limitaciones cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás."

En este sentido el Dictamen 4/2004 relativo al tratamiento de datos personales mediante vigilancia por videocámara, señalaba respecto a la proporcionalidad del recurso a la vigilancia por videocámara, "…que el circuito cerrado de televisión y otros sistemas similares de vigilancia por videocámara sólo podrán utilizarse con carácter subsidiario, es decir: con fines que realmente justifiquen el recurso a tales sistemas. (….).Deberá evitarse, por ejemplo, que un organismo administrativo pueda instalar equipos de vigilancia por videocámara en relación con infracciones de menor importancia (por ejemplo, para reforzar la prohibición de fumar en los colegios y otros lugares públicos o la prohibición de tirar colillas y papeles al suelo en los lugares públicos). Dicho de otro modo, es necesario aplicar, caso por caso, el *principio de idoneidad* con respecto a los fines perseguidos, lo que implica una especie de *obligación de minimización de los datos* por parte del responsable del tratamiento."

Por tanto, con carácter general no se entiende por esta Agencia que sea proporcionada la utilización en las aulas en las que se celebre los exámenes de la Universidad, de un sistema de videovigilancia que permitiera su grabación como una forma de seguimiento de la evaluación de los alumnos y evitar así conductas inapropiadas.

Por consiguiente, la existencia de un interés público no legitima cualquier tipo de tratamiento de datos personales, sino que deberá estarse, en primer lugar, a las condiciones que haya podido establecer el legislador, tal como prevé el propio artículo 6 del RGPD, en sus apartados 2 y 3, así como a los ya citados principios del artículo 5 del RGPD, especialmente a los de limitación de la finalidad y minimización de datos.

Y en el caso de que vayan a ser objeto de tratamiento alguno o algunos de los datos personales incluidos en las categorías especiales de datos a los que se refiere el artículo 9.1. del RGPD, que concurra alguna de las circunstancias contempladas en su apartado 2 que levante la prohibición de tratamiento de dichos datos, establecida con carácter general en su apartado 1.

III

En el presente caso, versando la consulta sobre técnicas de reconocimiento facial dirigidas a acreditar la identidad del alumno, nos encontraríamos ante el tratamiento de datos biométricos, tal y como los define el artículo 4.14 del RGPD:

> «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 confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos;

No obstante, hay que adelantar que el RGPD no parece considerar a todo tratamiento de datos biométricos como tratamiento de categorías especiales de datos, ya que el artículo 9.1. se refiere a los “datos biométricos dirigidos a identificar de manera unívoca a una persona física”, por lo que, de una interpretación conjunta de ambos preceptos parece dar a entender que los datos biométricos solo constituirían una categoría especial de datos en el caso de que se sometan a un tratamiento técnico específico dirigido a identificar de manera unívoca a una persona física. En este sentido, parece que igualmente se pronuncia el Considerando 51 al señalar 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”.

Con igual criterio, el Protocolo de enmienda al Convenio para la Protección de Individuos con respecto al procesamiento de datos personales, aprobada por el Comité de Ministros en su 128º período de sesiones en Elsinore el 18 de mayo de 2018 (Convenio 108+) incluye únicamente como categorías especiales de datos, en su artículo 6.1 a los datos biométricos dirigidos a la identificación unívoca de una persona (“biometric data uniquely identifying a person”), sin incluir la referencia a la autenticación.

Al objeto de aclarar las dudas interpretativas que surgen respecto a la consideración de los datos biométricos como categorías especiales de datos puede acudirse a la distinción entre identificación biométrica y verificación/autenticación biométrica que establecía el Grupo del Artículo 29 en su Dictamen 3/2012 sobre la evolución de las tecnologías biométricas:

> Identificación biométrica: la identificación de un individuo por un sistema biométrico es normalmente el proceso de comparar sus datos biométricos (adquiridos en el momento de la identificación) con una serie de plantillas biométricas almacenadas en una base de datos (es decir, un proceso de búsqueda de correspondencias uno-a-varios).
>
> Verificación/autenticación biométrica: la verificación de un individuo por un sistema biométrico es normalmente el proceso de comparación entre sus datos biométricos (adquiridos en el momento de la verificación) con una única plantilla biométrica almacenada en un dispositivo (es decir, un proceso de búsqueda de correspondencias uno-a-uno).

Esta misma diferenciación se recoge en el Libro blanco sobre la inteligencia artificial de la Comisión Europea:

> "En lo que se refiere al reconocimiento facial, por «identificación» se entiende que la plantilla de la imagen facial de una persona se compara con otras muchas plantillas almacenadas en una base de datos para averiguar si su imagen está almacenada en ella. La «autenticación» (o «verificación»), por su parte, se refiere habitualmente a la búsqueda de correspondencias entre dos plantillas concretas. Permite la comparación de dos plantillas biométricas que, en principio, se supone que pertenecen a la misma persona; así, las dos plantillas se comparan para determinar si la persona de las dos imágenes es la misma. Este procedimiento se emplea, por ejemplo, en las puertas de control automatizado de fronteras empleadas en los controles fronterizos de los aeropuertos".

Atendiendo a la citada distinción, puede interpretarse que, de acuerdo con el artículo 4 del RGPD, el concepto de dato biométrico incluiría ambos supuestos, tanto la identificación como la verificación/autenticación. Sin embargo, y con carácter general, los datos biométricos únicamente tendrán la consideración de categoría especial de datos en los supuestos en que se sometan a tratamiento técnico dirigido a la identificación biométrica (uno-a-varios) y no en el caso de verificación/autenticación biométrica (uno-a-uno).

No obstante, esta Agencia considera que se trata de una cuestión compleja, sometida a interpretación, respecto de la cual no se pueden extraer conclusiones generales, debiendo atenderse al caso concreto según los datos tratados, las técnicas empleadas para su tratamiento y la consiguiente injerencia en el derecho a la protección de datos, debiendo, en tanto en cuanto no se pronuncia al respecto el Comité Europeo de Protección de Datos o los órganos jurisdiccionales, adoptarse, en caso de duda, la interpretación más favorable para la protección de los derechos de los afectados.

En el presente caso, tal y como hemos señalado, la consultante no identifica las técnicas de tratamiento facial a la que se refiere la consulta. No obstante, tal y como ha informado al Gabinete Jurídico la Unidad de Evaluación y Estudios Tecnológicos, son diferentes las técnicas que se están empleando en el momento actual:

> "En el conjunto de consultas planteadas se establecen medidas para la identificación y control durante la prueba online que abarcan, desde las menos intrusivas a las más intrusivas:
>
> - Acceso a la imagen y micrófono del alumno, incluyendo

- o Grabación de la imagen y sonido del alumno durante el examen
- o Visualización del alumno multicámara, desde distintas perspectivas.
- o Grabaciones del entorno personal del alumno previa a la prueba y/o durante la prueba.

- Acceso al sistema del alumno
  - o Acceso a la pantalla del alumno
  - o Control del sistema del alumno (al menos bloqueando la ejecución de aplicaciones distintas a las aplicaciones docentes).
  - o Grabación de la interacción del alumno con el sistema

- Tratamiento de la información biométrica
  - o Identificación mediante reconocimiento facial y, además, otros parámetros biométricos del alumno (como perfil de mecanografía).
  - o Tratamiento de datos biométricos para perfilar actitudes, gestos, estados de ánimo o de ansiedad, etc".

Debiendo tenerse en cuenta que, tal y como se reconoce en la "Segunda Jornada Online para Compartición de Experiencias de Modelos de Evaluación" ya citada, las universidades están combinando diferentes sistemas para acreditar la identidad del alumno y evitar las posibles suplantaciones de identidad. Además, una de las características de los sistemas de e-proctoring existentes en el mercado es que garantizan la identificación del alumno mediante el reconocimiento facial, evitando la suplantación de su identidad, no solo en el momento inicial, sino a lo largo del desarrollo de toda la actividad, para lo cual se graba la misma y se van realizando diferentes capturas que se comparan con la información biométrica previamente almacenada en sus bases de datos. Asimismo, dichos sistemas incluyen, tal y como se ha indicado, el tratamiento de otro tipo de datos biométricos (como las pulsaciones en el teclado) y de datos no biométricos, como la grabación del entorno en el que se encuentra el alumno, así como el acceso al micrófono para la grabación de sonidos.

Por tanto, atendiendo a las circunstancias concretas, que implican el tratamiento de diferentes tipos de datos biométricos y en los que el reconocimiento facial no se realiza en un momento determinado sino que se realiza de manera continuada, lo que puede implicar, asimismo, el tratamiento de los datos biométricos de un tercero para su comparación con los del alumno al objeto de identificar una posible suplantación, debe concluirse que los procesos de reconocimiento facial empleados para la realización de evaluaciones online implican el tratamiento de datos biométricos con la finalidad de identificar unívocamente a una persona física.

En este mismo sentido, cabe recordar que el Supervisor Europeo de Protección de Datos, en sus “Guidelines 3/2019 on processing of personal data through video devices" de 10 de julio de 2019 considera el empleo de videovigilancia con reconocimiento facial como categoría especial de datos del artículo 9 del RGPD:

> 76. The use of video surveillance including biometric recognition functionality installed by private entities for their own purposes (e.g. marketing, statistical, or even security) will, in most cases, require explicit consent of all data subjects (Article 9 (2) (a)), however another suitable exception in Article 9 could also be applicable.
>
> Example: To improve its service a private company replaces passenger identification check points within an airport (luggage drop-off, boarding) with video surveillance systems that use facial recognition techniques to verify the identity of the passengers that have chosen to consent to such a procedure. Since the processing falls under Article 9, the passengers, who will have previously given their explicit and informed consent, will have to enlist themselves at for example an automatic terminal in order to create and register their facial template associated with their boarding pass and identity.

Por ello, esta Agencia comparte el criterio de la consultante, en el sentido de que **los sistemas de reconocimiento facial objeto de la consulta implican el tratamiento de categoría especiales de datos**.

IV

Por consiguiente, para que sea lícito el tratamiento de los datos biométricos, debe concurrir alguna de las excepciones que levanten la prohibición de su tratamiento, conforme al apartado 2 del artículo 9 del RGPD, planteándose en la consulta, en primer término, la posibilidad de que el alumno pudiera prestar su consentimiento a su tratamiento y en qué medida dicho consentimiento podría considerarse libre.

El primer supuesto que prevé el artículo 9.2. para poder proceder al tratamiento de categorías especiales de datos es el consentimiento del afectado:

> a) el interesado dio su consentimiento explícito para el tratamiento de dichos 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;

Haciendo uso de la habilitación establecida en el citado precepto, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, en su artículo 9.1, no ha incluido entre los supuestos en que el consentimiento, por si solo, no bastará para levantar la prohibición a los datos biométricos:

> Artículo 9. Categorías especiales de datos.
>
> 1. A los efectos del artículo 9.2.a) del Reglamento (UE) 2016/679, a fin de evitar situaciones discriminatorias, el solo consentimiento del afectado no bastará para levantar la prohibición del tratamiento de datos cuya finalidad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias u origen racial o étnico.
>
> Lo dispuesto en el párrafo anterior no impedirá el tratamiento de dichos datos al amparo de los restantes supuestos contemplados en el artículo 9.2 del Reglamento (UE) 2016/679, cuando así proceda.

Por consiguiente, el consentimiento del alumno podría permitir el tratamiento de sus datos biométricos, siempre que concurran los requisitos establecidos en el RGPD, que define al consentimiento en su artículo 4.11 como “toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen”.

Dicho precepto no hace sino recoger los requisitos de un consentimiento válido que se habían venido perfilando por el Grupo del 29, especialmente en su Dictamen 15/2011 sobre la definición del consentimiento, garantizando que el interesado tenga el control sobre sus datos. Como señala el Grupo del 29 en sus Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679 adoptadas el 28 de noviembre de 2017, si no se cumple plenamente con el RGPD “el control del interesado será meramente ilusorio y el consentimiento no será una base jurídica válida para el tratamiento, lo que convertirá dicha actividad de tratamiento en una actividad ilícita”, teniendo en cuenta, además, que “los requisitos estipulados en el RGPD para obtener un consentimiento válido se aplican a situaciones que entran dentro del ámbito de aplicación de la Directiva sobre la privacidad y las comunicaciones electrónicas”.

El principal problema que plantea el consentimiento en el presente caso, atendiendo a que el alumno no se encuentra en situación de igualdad con la universidad en la que estudia, es el relativo al requisito de que el mismo sea libre.

A este respecto, el Considerando 42 del RGPD destaca que “El consentimiento no debe considerarse libremente prestado cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno”.

Y el Considerando 43, pensando en situaciones de desigualdad como la presente, indica lo siguiente:

> "Para garantizar que el consentimiento se haya dado libremente, este no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibro claro entre el interesado y el responsable del tratamiento, en particular cuando dicho responsable sea una autoridad pública y sea por lo tanto improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular. Se presume que el consentimiento no se ha dado libremente cuando no permita autorizar por separado las distintas operaciones de tratamiento de datos personales pese a ser adecuado en el caso concreto, o cuando el cumplimiento de un contrato, incluida la prestación de un servicio, sea dependiente del consentimiento, aún cuando este no sea necesario para dicho cumplimiento".

Asimismo, el artículo 7.4. del RGPD dispone que "Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato".

De acuerdo con las Directrices sobre el consentimiento del Grupo del 29, ya citadas:

> "El término «libre» implica elección y control reales por parte de los interesados. Como norma general, el RGPD establece que, si el sujeto no es realmente libre para elegir, se siente obligado a dar su consentimiento o sufrirá consecuencias negativas si no lo da, entonces el consentimiento no puede considerarse válido.
>
> […]
>
> A la hora de valorar si el consentimiento se ha dado libremente, deben considerarse también las situaciones concretas en las que el consentimiento se supedita a la ejecución de contratos o a la prestación de un servicio tal y como se describe en el artículo 7, apartado 4. El artículo 7, apartado 4, se ha redactado de manera no exhaustiva mediante el uso de la expresión «entre otras cosas», lo que significa que puede haber otras circunstancias que entren en el ámbito de aplicación de esta disposición. En términos generales, el consentimiento quedará invalidado por cualquier influencia o presión inadecuada ejercida sobre el interesado (que puede manifestarse de formas muy distintas) que impida que este ejerza su libre voluntad.

En relación con las situaciones de desequilibrio de poder, las Directrices se refieren al supuesto de autoridades públicas y empleadores. Centrándonos en las primeras, cuyas consideraciones, teniendo en cuenta la configuración de la educación superior como un servicio público, serían trasladables al supuesto que nos ocupa, señala lo siguiente:

> El considerando 43 indica claramente que no es probable que las autoridades públicas puedan basarse en el consentimiento para realizar el tratamiento de datos ya que cuando el responsable del tratamiento es una autoridad pública, siempre hay un claro desequilibrio de poder en la relación entre el responsable del tratamiento y el interesado. Queda también claro en la mayoría de los casos que el interesado no dispondrá de alternativas realistas para aceptar el tratamiento (las condiciones de tratamiento) de dicho responsable. El GT29 considera que hay otras bases jurídicas que son, en principio, más adecuadas para el tratamiento de datos por las autoridades públicas15.
> Sin perjuicio de estas consideraciones generales, el uso del consentimiento como una base jurídica para el tratamiento de datos por parte de las autoridades públicas no queda totalmente excluido en virtud del marco jurídico del RGPD.

Y entre los ejemplos que citan las Directrices como muestra de que el uso del consentimiento puede ser adecuado en determinadas circunstancias respecto de los tratamientos realizados por autoridades públicas incluye el siguiente:

> “Una escuela pública pide a sus alumnos el consentimiento para utilizar sus fotografías en una revista escolar impresa. El consentimiento en estas situaciones sería una elección real siempre que no se negara a los alumnos la educación u otros servicios y ellos pudieran negarse al uso de dichas fotografías sin sufrir ningún perjuicio”

Por último, concluyen las citadas Directrices que:

> “Los desequilibrios de poder no se limitan a las autoridades públicas y a los empleadores, sino que también pueden producirse en otras situaciones. Como ha subrayado el GT29 en diversos dictámenes, el consentimiento solo puede ser válido si el interesado puede realmente elegir y no existe riesgo de engaño, intimidación, coerción o consecuencias negativas importantes (por ejemplo, costes adicionales sustanciales) si no da su consentimiento. El consentimiento no será libre en aquellos casos en los que exista un elemento de compulsión, presión o incapacidad para ejercer la libre voluntad”.

Partiendo de dichos criterios, **la posibilidad de admitir un consentimiento libre de los alumnos que permitiera el empleo de técnicas de reconocimiento facial al objeto de tratar sus datos biométricos en las evaluaciones online requeriría que a los mismos se les ofreciera la posibilidad de realizar dichas evaluaciones en una situación equiparable en la que no fuera necesario su tratamiento,** como pudiera ser la realización de la misma actividad presencialmente, u ofreciendo otras alternativas que no requieran el tratamiento de sus datos biométricos y que fueran equiparables en cuanto a su duración y dificultad a las que se realicen mediante el empleo del reconocimiento facial; ya que en otro caso, como por ejemplo, si las actividades alternativas fueran más gravosas o implicaran una mayor dificultad, el consentimiento no podría considerarse libremente prestado. **Y lo que no sería admisible, en ningún caso, es que como consecuencia de la denegación del consentimiento se denegara la posibilidad de matriculación o de acceder a la evaluación o cualquier otra consecuencia negativa importante para el alumno.**

Corresponde, por ende, a las universidades, en virtud del principio de autonomía universitaria y en cuanto responsables del tratamiento, y sin perjuicio de su supervisión por las agencias de calidad, determinar en sus normas de evaluación y en sus planes de formación los procedimientos de evaluación que acrediten la igualdad entre los alumnos que consientan el tratamiento de sus datos biométricos y los que no lo hagan. Únicamente de este modo, el consentimiento podría legitimar de dicho tratamiento.

Todo ello sin perjuicio de que el consentimiento deba cumplir, asimismo, los demás requisitos que establece el RGPD: expreso, específico, informado y revocable.

V

La siguiente cuestión que se plantea en la consulta es si el tratamiento de los datos biométricos por los sistemas de reconocimiento facial en los procesos de evaluación online podría ampararse en la existencia de un interés público esencial conforme al artículo 9.2.g) del RGPD:

> g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del 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.

Tal y como señalábamos anteriormente, el tratamiento de datos personales necesarios para la prestación del servicio público de educación superior se legitima, con carácter general, en la existencia de un interés público al amparo de lo previsto en el artículo 6.1.e) del RGPD. Sin embargo, tratándose de categorías especiales de datos, el supuesto contemplado en la letra g) del artículo 9.2. no se refiere solo a la existencia de un interés público, tal y como hace en muchos otros de sus preceptos el RGPD, sino que es el único precepto del RGPD que requiere que el mismo sea "esencial", adjetivo que viene a cualificar dicho interés público, habida cuenta de la importancia y necesidad de mayor protección de los datos tratados.

Dicho precepto encuentra su precedente en el artículo 8.4 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos: "4. Siempre que dispongan las garantías adecuadas, los Estados miembros podrán, por motivos de interés público importantes, establecer otras excepciones, además de las previstas en el apartado 2, bien mediante su legislación nacional, bien por decisión de la autoridad de control". No obstante, de su lectura resulta un mayor rigor en a nueva regulación por el RGPD, ya que se sustituye el adjetivo "importantes" por "esencial" y no se permite que la excepción pueda establecerse por las autoridades de control.

En relación con lo que debe entenderse por interés público esencial, debe tenerse igualmente en cuenta la Jurisprudencia del Tribunal Europeo de Derechos Humanos, que al amparo del artículo 8 del Convenio Europeo de Derechos Humanos, viene considerando que el tratamiento de datos personales constituye una injerencia lícita en el derecho del respeto de la vida privada y sólo puede llevarse a cabo si se realiza de conformidad con la ley, sirve a un fin legítimo, respeta la esencia de los derechos y libertades fundamentales y es necesario y proporcionado en una sociedad democrática para alcanzar un fin legítimo (D.L. contra Bulgaria, nº 7472/14, 19 de mayo de 2016, Dragojević contra Croacia, nº 68955/11, 15 de enero de 2015, Peck contra Reino Unido, nº 44647/98, 28 de enero de 2003, Leander contra Suecia, n.o 9248/81, 26 de marzo de 1987, entre otras). Como señala en la última sentencia citada, «el concepto de necesidad implica que la injerencia responda a una necesidad social acuciante y, en particular, que sea proporcionada con el fin legítimo que persigue».

Asimismo, debe tenerse en cuenta la doctrina del Tribunal Constitucional respecto a las restricciones al derecho fundamental a la protección de datos, que sintetiza en su sentencia 292/2000, de 30 de noviembre, en la que después de configurar el derecho fundamental a la protección de datos personales como un derecho autónomo e independiente que consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también

permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso, analiza los límites del mismo, señalando en lo siguiente:

> Más concretamente, en las Sentencias mencionadas relativas a la protección de datos, este Tribunal ha declarado que el derecho a la protección de datos no es ilimitado, y aunque la Constitución no le imponga expresamente límites específicos, ni remita a los Poderes Públicos para su determinación como ha hecho con otros derechos fundamentales, no cabe duda de que han de encontrarlos en los restantes derechos fundamentales y bienes jurídicos constitucionalmente protegidos, pues así lo exige el principio de unidad de la Constitución (SSTC 11/1981, de 8 de abril, F. 7; 196/1987, de 11 de diciembre [RTC 1987, 196] , F. 6; y respecto del art. 18, la STC 110/1984, F. 5). Esos límites o bien pueden ser restricciones directas del derecho fundamental mismo, a las que antes se ha aludido, o bien pueden ser restricciones al modo, tiempo o lugar de ejercicio del derecho fundamental. En el primer caso, regular esos límites es una forma de desarrollo del derecho fundamental. En el segundo, los límites que se fijan lo son a la forma concreta en la que cabe ejercer el haz de facultades que compone el contenido del derecho fundamental en cuestión, constituyendo una manera de regular su ejercicio, lo que puede hacer el legislador ordinario a tenor de lo dispuesto en el art. 53.1 CE. La primera constatación que debe hacerse, que no por evidente es menos capital, es que la Constitución ha querido que la Ley, y sólo la Ley, pueda fijar los límites a un derecho fundamental. Los derechos fundamentales pueden ceder, desde luego, ante bienes, e incluso intereses constitucionalmente relevantes, siempre que el recorte que experimenten sea necesario para lograr el fin legítimo previsto, proporcionado para alcanzarlo y, en todo caso, sea respetuoso con el contenido esencial del derecho fundamental restringido (SSTC 57/1994, de 28 de febrero [RTC 1994, 57] , F. 6; 18/1999, de 22 de febrero [RTC 1999, 18] , F. 2).
>
> Justamente, si la Ley es la única habilitada por la Constitución para fijar los límites a los derechos fundamentales y, en el caso presente, al derecho fundamental a la protección de datos, y esos límites no pueden ser distintos a los constitucionalmente previstos, que para el caso no son otros que los derivados de la coexistencia de este derecho fundamental con otros derechos y bienes jurídicos de rango constitucional, el apoderamiento legal que permita a un Poder Público recoger, almacenar, tratar, usar y, en su caso, ceder datos personales, sólo está justificado si responde a la protección de otros derechos fundamentales o bienes constitucionalmente protegidos. Por tanto, si aquellas operaciones con los datos personales de una persona no se realizan con estricta observancia de las normas que lo regulan, se vulnera el derecho a la protección de datos, pues se le imponen límites constitucionalmente ilegítimos, ya sea a su contenido o al ejercicio del haz de facultades que

lo componen. Como lo conculcará también esa Ley limitativa si regula los límites de forma tal que hagan impracticable el derecho fundamental afectado o ineficaz la garantía que la Constitución le otorga. Y así será cuando la Ley, que debe regular los límites a los derechos fundamentales con escrupuloso respeto a su contenido esencial, se limita a apoderar a otro Poder Público para fijar en cada caso las restricciones que pueden imponerse a los derechos fundamentales, cuya singular determinación y aplicación estará al albur de las decisiones que adopte ese Poder Público, quien podrá decidir, en lo que ahora nos interesa, sobre la obtención, almacenamiento, tratamiento, uso y cesión de datos personales en los casos que estime convenientes y esgrimiendo, incluso, intereses o bienes que no son protegidos con rango constitucional […]". (Fundamento Jurídico 11)

"De un lado, porque si bien este Tribunal ha declarado que la Constitución no impide al Estado proteger derechos o bienes jurídicos a costa del sacrificio de otros igualmente reconocidos y, por tanto, que el legislador pueda imponer limitaciones al contenido de los derechos fundamentales o a su ejercicio, también hemos precisado que, en tales supuestos, esas limitaciones han de estar justificadas en la protección de otros derechos o bienes constitucionales (SSTC 104/2000, de 13 de abril [RTC 2000, 104] , F. 8 y las allí citadas) y, además, han de ser proporcionadas al fin perseguido con ellas (SSTC 11/1981, F. 5, y 196/1987, F. 6). Pues en otro caso incurrirían en la arbitrariedad proscrita por el art. 9.3 CE.

De otro lado, aun teniendo un fundamento constitucional y resultando proporcionadas las limitaciones del derecho fundamental establecidas por una Ley (STC 178/1985 [RTC 1985, 178]), éstas pueden vulnerar la Constitución si adolecen de falta de certeza y previsibilidad en los propios límites que imponen y su modo de aplicación. Conclusión que se corrobora en la jurisprudencia del Tribunal Europeo de Derechos Humanos que ha sido citada en el F. 8 y que aquí ha de darse por reproducida. Y ha de señalarse, asimismo, que no sólo lesionaría el principio de seguridad jurídica (art. 9.3 CE), concebida como certeza sobre el ordenamiento aplicable y expectativa razonablemente fundada de la persona sobre cuál ha de ser la actuación del poder aplicando el Derecho (STC 104/2000, F. 7, por todas), sino que al mismo tiempo dicha Ley estaría lesionando el contenido esencial del derecho fundamental así restringido, dado que la forma en que se han fijado sus límites lo hacen irreconocible e imposibilitan, en la práctica, su ejercicio (SSTC 11/1981, F. 15; 142/1993, de 22 de abril [RTC 1993, 142] , F. 4, y 341/1993, de 18 de noviembre [RTC 1993, 341] , F. 7). De suerte que la falta de precisión de la Ley en los presupuestos materiales de la limitación de un derecho fundamental es susceptible de generar una indeterminación sobre los casos a los que se aplica tal restricción. Y al

producirse este resultado, más allá de toda interpretación razonable, la Ley ya no cumple su función de garantía del propio derecho fundamental que restringe, pues deja que en su lugar opere simplemente la voluntad de quien ha de aplicarla, menoscabando así tanto la eficacia del derecho fundamental como la seguridad jurídica […]". (FJ 15).

"Más concretamente, en relación con el derecho fundamental a la intimidad hemos puesto de relieve no sólo la necesidad de que sus posibles limitaciones estén fundadas en una previsión legal que tenga justificación constitucional y que sean proporcionadas (SSTC 110/1984, F. 3, y 254/1993, F. 7) sino que la Ley que restrinja este derecho debe expresar con precisión todos y cada uno de los presupuestos materiales de la medida limitadora. De no ser así, mal cabe entender que la resolución judicial o el acto administrativo que la aplique estén fundados en la Ley, ya que lo que ésta ha hecho, haciendo dejación de sus funciones, es apoderar a otros Poderes Públicos para que sean ellos quienes fijen los límites al derecho fundamental (SSTC 37/1989, de 15 de febrero [RTC 1989, 37], y 49/1999, de 5 de abril [RTC 1999, 49]).
De igual modo, respecto al derecho a la protección de datos personales cabe estimar que la legitimidad constitucional de la restricción de este derecho no puede estar basada, por sí sola, en la actividad de la Administración Pública. Ni es suficiente que la Ley apodere a ésta para que precise en cada caso sus límites, limitándose a indicar que deberá hacer tal precisión cuando concurra algún derecho o bien constitucionalmente protegido. Es el legislador quien debe determinar cuándo concurre ese bien o derecho que justifica la restricción del derecho a la protección de datos personales y en qué circunstancias puede limitarse y, además, es él quien debe hacerlo mediante reglas precisas que hagan previsible al interesado la imposición de tal limitación y sus consecuencias. Pues en otro caso el legislador habría trasladado a la Administración el desempeño de una función que sólo a él compete en materia de derechos fundamentales en virtud de la reserva de Ley del art. 53.1 CE, esto es, establecer claramente el límite y su regulación. […] (FJ 16)".

Asimismo, nuestro Tribunal Constitucional ha tenido ya la ocasión de pronunciarse específicamente sobre el artículo 9.2.g) del RGPD, como consecuencia de la impugnación del artículo 58 bis de la Ley Orgánica 5/1985, de 19 de junio, del Régimen Electoral General, introducido por la disposición final tercera de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, relativo a la legitimación de la recopilación de datos personales relativos a las opiniones políticas de las personas que lleven a cabo los partidos políticos en el marco de sus actividades electorales, precepto que fue declarado inconstitucional por la Sentencia num. 76/2019 de 22 mayo.

Dicha sentencia analiza, en primer término, el régimen jurídico al que se encuentra sometido el tratamiento de las categorías especiales de datos en el RGPD:

> De acuerdo con el apartado 1 del art. 9 RGPD, está prohibido el tratamiento de datos personales que revelen las opiniones políticas, del mismo modo que lo está el tratamiento de datos personales que revelen el origen étnico o racial, las convicciones religiosas o filosóficas o la afiliación sindical y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera 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. No obstante, el apartado 2 del mismo precepto autoriza el tratamiento de todos esos datos cuando concurra alguna de las diez circunstancias allí previstas [letras a) a j)]. Algunas de esas circunstancias tienen un ámbito de aplicación acotado (laboral, social, asociativo, sanitario, judicial, etc.) o responden a una finalidad determinada, por lo que, en sí mismas, delimitan los tratamientos específicos que autorizan como excepción a la regla general. Además, la eficacia habilitante de varios de los supuestos allí previstos está condicionada a que el Derecho de la Unión o el de los Estados miembros los prevean y regulen expresamente en su ámbito de competencias: es el caso de las circunstancias recogidas en las letras a), b), g), h), i) y j).
>
> El tratamiento de las categorías especiales de datos personales es uno de los ámbitos en los que de manera expresa el Reglamento General de Protección de Datos ha reconocido a los Estados miembros "margen de maniobra" a la hora de "especificar sus normas", tal como lo califica su considerando 10. **Este margen de configuración legislativa se extiende tanto a la determinación de las causas habilitantes para el tratamiento de datos personales especialmente protegidos -es decir, a la identificación de los fines de interés público esencial y la apreciación de la proporcionalidad del tratamiento al fin perseguido, respetando en lo esencial el derecho a la protección de datos- como al establecimiento de "medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado" [art. 9.2 g) RGPD]. El Reglamento contiene, por tanto, una obligación concreta de los Estados miembros de establecer tales garantías, en el caso de que habiliten para tratar los datos personales especialmente protegidos.**

En relación con el primero de los requisitos exigidos por el artículo 9.2.g), la invocación de un interés público esencial y la necesaria especificación del mismo, el Alto Tribunal recuerda lo señalado en su sentencia 292/2000 en la que se rechazaba que la identificación de los fines legítimos de la restricción pudiera realizarse mediante conceptos genéricos o fórmulas vagas, considerando que la restricción del derecho fundamental a la protección de

datos personales no puede estar basada, por sí sola, en la invocación genérica de un indeterminado "interés público" :

> En la ya citada STC 292/2000 (RTC 2000, 292) , en la que también se enjuició una injerencia legislativa en el derecho a la protección de datos personales, rechazamos que la identificación de los fines legítimos de la restricción pudiera realizarse mediante conceptos genéricos o fórmulas vagas:
> "16. [...] De igual modo, respecto al derecho a la protección de datos personales cabe estimar que la legitimidad constitucional de la restricción de este derecho no puede estar basada, por sí sola, en la actividad de la Administración Pública. Ni es suficiente que la Ley apodere a ésta para que precise en cada caso sus límites, limitándose a indicar que deberá hacer tal precisión cuando concurra algún derecho o bien constitucionalmente protegido. Es el legislador quien debe determinar cuándo concurre ese bien o derecho que justifica la restricción del derecho a la protección de datos personales y en qué circunstancias puede limitarse y, además, es él quien debe hacerlo mediante reglas precisas que hagan previsible al interesado la imposición de tal limitación y sus consecuencias. Pues en otro caso el legislador habría trasladado a la Administración el desempeño de una función que sólo a él compete en materia de derechos fundamentales en virtud de la reserva de Ley del art. 53.1 CE, esto es, establecer claramente el límite y su regulación.
> 17. En el caso presente, el empleo por la LOPD (RCL 2018, 1629) en su art. 24.1 de la expresión "funciones de control y verificación", abre un espacio de incertidumbre tan amplio que provoca una doble y perversa consecuencia. De un lado, al habilitar la LOPD a la Administración para que restrinja derechos fundamentales invocando semejante expresión está renunciando a fijar ella misma los límites, apoderando a la Administración para hacerlo. Y de un modo tal que, como señala el Defensor del Pueblo, permite reconducir a las mismas prácticamente toda actividad administrativa, ya que toda actividad administrativa que implique entablar una relación jurídica con un administrado, que así será prácticamente en todos los casos en los que la Administración necesite de datos personales de alguien, conllevará de ordinario la potestad de la Administración de verificar y controlar que ese administrado ha actuado conforme al régimen jurídico administrativo de la relación jurídica entablada con la Administración. Lo que, a la vista del motivo de restricción del derecho a ser informado del art. 5 LOPD, deja en la más absoluta incertidumbre al ciudadano sobre en qué casos concurrirá esa circunstancia (si no en todos) y sume en la ineficacia cualquier mecanismo de tutela jurisdiccional que deba enjuiciar semejante supuesto de restricción de derechos fundamentales sin otro criterio complementario que venga en ayuda de su control de la actuación administrativa en esta materia.

Iguales reproches merece, asimismo, el empleo en el art. 24.2 LOPD de la expresión "interés público" como fundamento de la imposición de límites a los derechos fundamentales del art. 18.1 y 4 CE, pues encierra un grado de incertidumbre aún mayor. Basta reparar en que toda actividad administrativa, en último término, persigue la salvaguardia de intereses generales, cuya consecución constituye la finalidad a la que debe servir con objetividad la Administración con arreglo al art. 103.1 CE."

Esta argumentación es plenamente trasladable al presente enjuiciamiento. De igual modo, por tanto, debemos concluir que la legitimidad constitucional de la restricción del derecho fundamental a la protección de datos personales no puede estar basada, por sí sola, en la invocación genérica de un indeterminado "interés público". Pues en otro caso el legislador habría trasladado a los partidos políticos -a quienes la disposición impugnada habilita para recopilar datos personales relativos a las opiniones políticas de las personas en el marco de sus actividades electorales- el desempeño de una función que solo a él compete en materia de derechos fundamentales en virtud de la reserva de Ley del art. 53.1 CE, esto es, establecer claramente sus límites y su regulación.

Tampoco puede aceptarse, por igualmente imprecisa, la finalidad aducida por el abogado del Estado, que se refiere al funcionamiento del sistema democrático, pues también encierra un grado elevado de incertidumbre y puede suponer un razonamiento circular. Por un lado, los partidos políticos son de por sí "cauces necesarios para el funcionamiento del sistema democrático" (por todas, STC 48/2003, de 12 de marzo (RTC 2003, 48) , FJ 5); y, por otro lado, todo el funcionamiento del sistema democrático persigue, en último término, la salvaguardia de los fines, valores y bienes constitucionales, pero ello no alcanza a identificar la razón por la cual haya de restringirse el derecho fundamental afectado.

Finalmente, debe precisarse que no es necesario que se pueda sospechar, con mayor o menor fundamento, que la restricción persiga una finalidad inconstitucional, o que los datos que se recopilen y procesen resultarán lesivos para la esfera privada y el ejercicio de los derechos de los particulares. Es suficiente con constatar que, al no poderse identificar con la suficiente precisión la finalidad del tratamiento de datos, tampoco puede enjuiciarse el carácter constitucionalmente legítimo de esa finalidad, ni, en su caso, la proporcionalidad de la medida prevista de acuerdo con los principios de idoneidad, necesidad y proporcionalidad en sentido estricto.

Por otro lado, en cuanto a las garantías que debe adoptar el legislador, la citada sentencia núm. 76/2019 de 22 mayo, después de recordar que “A la vista de los potenciales efectos intrusivos en el derecho fundamental afectado que resultan del tratamiento de datos personales, la jurisprudencia de este Tribunal le exige al legislador que, además de cumplir los requisitos

anteriormente mencionados, también establezca garantías adecuadas de tipo técnico, organizativo y procedimental, que prevengan los riesgos de distinta probabilidad y gravedad y mitiguen sus efectos, pues solo así se puede procurar el respeto del contenido esencial del propio derecho fundamental", analiza cuál es la norma que debe contener las citadas garantías:

> "Por tanto, la resolución de la presente impugnación exige que aclaremos una duda suscitada con respecto al alcance de nuestra doctrina sobre las garantías adecuadas, que consiste en determinar si las garantías adecuadas frente al uso de la informática deben contenerse en la propia ley que autoriza y regula ese uso o pueden encontrarse también en otras fuentes normativas.
> La cuestión solo puede tener una respuesta constitucional. La previsión de las garantías adecuadas no puede deferirse a un momento posterior a la regulación legal del tratamiento de datos personales de que se trate. Las garantías adecuadas deben estar incorporadas a la propia regulación legal del tratamiento, ya sea directamente o por remisión expresa y perfectamente delimitada a fuentes externas que posean el rango normativo adecuado. Solo ese entendimiento es compatible con la doble exigencia que dimana del art. 53.1 CE (RCL 1978, 2836) para el legislador de los derechos fundamentales: la reserva de ley para la regulación del ejercicio de los derechos fundamentales reconocidos en el capítulo segundo del título primero de la Constitución y el respeto del contenido esencial de dichos derechos fundamentales.
> Según reiterada doctrina constitucional, la reserva de ley no se limita a exigir que una ley habilite la medida restrictiva de derechos fundamentales, sino que también es preciso, conforme tanto a exigencias denominadas -unas veces- de predeterminación normativa y -otras- de calidad de la ley como al respeto al contenido esencial del derecho, que en esa regulación el legislador, que viene obligado de forma primaria a ponderar los derechos o intereses en pugna, predetermine los supuestos, las condiciones y las garantías en que procede la adopción de medidas restrictivas de derechos fundamentales. Ese mandato de predeterminación respecto de elementos esenciales, vinculados también en último término al juicio de proporcionalidad de la limitación del derecho fundamental, no puede quedar deferido a un ulterior desarrollo legal o reglamentario, ni tampoco se puede dejar en manos de los propios particulares" (FJ 8).

Por consiguiente, el tratamiento de datos biométricos al amparo del artículo 9.2.g) requiere que esté previsto en una norma de derecho europeo o nacional, debiendo tener en este último caso dicha norma, según la doctrina constitucional citada y lo previsto en el artículo 9.2 de la LOPDGDD, rango de ley. Dicha ley deberá, además especificar el interés público esencial que justifica la restricción del derecho a la protección de datos personales y en qué circunstancias puede limitarse, estableciendo las reglas precisas que hagan previsible al interesado la imposición de tal

limitación y sus consecuencias, sin que sea suficiente, a estos efectos, la invocación genérica de un interés público. Y dicha ley deberá establecer, además, las garantías adecuadas de tipo técnico, organizativo y procedimental, que prevengan los riesgos de distinta probabilidad y gravedad y mitiguen sus efectos.

Además, dicha ley deberá respetar en todo caso el principio de proporcionalidad, tal y como recuerda la Sentencia del Tribunal Constitucional 14/2003, de 28 de enero:

> "En otras palabras, de conformidad con una reiterada doctrina de este Tribunal, la constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad. A los efectos que aquí importan basta con recordar que, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres requisitos o condiciones siguientes: si la 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, por 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; SSTC 66/1995, de 8 de mayo [RTC 1995, 66] , F. 5; 55/1996, de 28 de marzo [RTC 1996, 55] , FF. 7, 8 y 9; 270/1996, de 16 de diciembre [RTC 1996, 270] , F. 4.e; 37/1998, de 17 de febrero [RTC 1998, 37] , F. 8; 186/2000, de 10 de julio [RTC 2000, 186] , F. 6)."

Aplicando la citada doctrina al presente caso, debe partirse del reconocimiento del derecho a la educación como un derecho fundamental en el artículo 27 de la Constitución, configurando el artículo 1 de la Ley Orgánica de Universidades a la educación superior como un servicio público que se realiza por las universidades mediante la investigación, la docencia y el estudio.

En relación con la evaluación de los alumnos, el artículo 46.3. de la LOU, señala lo siguiente:

> 3. Las Universidades establecerán los procedimientos de verificación de los conocimientos de los estudiantes. En las Universidades públicas, el Consejo Social, previo informe del Consejo de Universidades, aprobará las normas que regulen el progreso y la permanencia en la Universidad de los estudiantes, de acuerdo con las características de los respectivos estudios.

Dicho precepto, y atendiendo a lo planteado en la consulta, se considera insuficiente para permitir la utilización de técnicas de reconocimiento facial en

los procesos de evaluación, al no cumplir los requisitos anteriormente señalados, siendo necesario que se aprobara una norma con rango de ley que justificara específicamente en qué medida y en qué supuestos, la identificación de los alumnos mediante el empleo de la biometría respondería a un interés público esencial, definiendo dicha norma legal, previa ponderación por el legislador de los intereses en pugna atendiendo al principio de proporcionalidad, todos y cada uno de los presupuestos materiales de la medida limitadora mediante reglas precisas, que hagan previsible al interesado la imposición de tal limitación y sus consecuencias, y estableciendo las garantías técnicas, organizativas y procedimentales adecuadas, que prevengan los riesgos de distinta probabilidad y gravedad y mitiguen sus efectos.

Dicha norma, en el caso de tramitarse, deberá ser preceptivamente informada por esta Agencia, momento en el cual podría valorarse si la misma se ajusta a los criterios señalados, sin que, apriorísticamente, se puede establecer un criterio taxativo por nuestra parte. No obstante, si puede adelantarse que, atendiendo al principio de proporcionalidad y al juicio de necesidad, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia, la existencia de otras medidas que permiten acreditar la identidad de los alumnos y supervisar los procesos de evaluación con una menor intrusión en el derecho de los afectados, exigiría una especial justificación de la necesidad de optar por el reconocimiento facial respecto de dichas otras medidas.

Es en relación con este último aspecto, en el que podría tener una especial incidencia la situación generada como consecuencia del Covid-19 y de la declaración del estado de alarma, en la que podría valorarse la prevalencia del reconocimiento facial frente a otras medidas, atendiendo a que una de las mismas, consistente en la evaluación presencial, pudiera no ser posible, tal y como ocurre en el momento actual. Pero sin que, a juicio de esta Agencia, pudiera optarse por la misma con carácter general, sino que debería quedar limitada a aquellas enseñanzas y asignaturas concretas que, por su importancia, complejidad u otras circunstancias de especial incidencia, no aconsejaran acudir a otras opciones, como la evaluación continua, o hicieran excesivamente gravoso la adopción de otros medios como el control por videocámara o la realización de exámenes orales.

VI

Por último, tanto en el caso de que se procediera al reconocimiento facial sobre la base de un consentimiento libre de los afectados como en el caso de que se apruebe una norma con rango de ley que lo ampare conforme al artículo 9.2.g), deberán adoptarse todas las medidas que garanticen que el tratamiento es conforme a la normativa sobre protección de datos personales, las cuales, en el último caso, deberán recogerse en la propia norma legal, sin perjuicio de su especificación por el responsable.

Para la adopción de dichas medidas, debe atenderse al principio de responsabilidad proactiva y de protección de datos desde el diseño por defecto, para lo que resulta esencial la realización del correspondiente análisis de riesgos, conforme al artículo 24 del RGPD.

Por otro lado, hay que tener en cuenta que nos encontramos ante tratamientos de categorías especiales de datos, sujetos a una especial protección, **cuyo tratamiento en el presente caso va a implicar un alto riesgo que haría necesario la realización de una evaluación de impacto en la protección de datos**, tal y como señala la Unidad de Evaluación y Estudios Tecnológicos:

"El tratamiento biométrico puede abarcar reconocimiento y análisis facial, de pulsaciones de teclado, de movimiento de ratón y otros no identificados en este informe.

El análisis de la legitimidad del tratamiento biométrico ha de estar basado en una base legal, pero también si el tratamiento es necesario, proporcional y se puede llevar a cabo con un riesgo bajo para los derechos y libertades de los interesados.

El tratamiento biométrico puede realizar dos niveles de tratamiento:

- Identificación
- Perfilado del alumno, como funcionalidad añadida a la anterior.

Ambos tratamientos utilizan técnicas de inteligencia artificial. Como se ha señalado anteriormente, hay que tener presente que estos tratamientos conllevan unos riesgos para los derechos y libertades adicionales. Por lo tanto, antes de cualquier apreciación sobre los mismos, es necesario auditar su funcionamiento, no de forma aislada, sino en el marco del tratamiento concreto en el que se va a emplear.

En cuanto ese tratamiento está orientado a la identificación de la persona, hay que considerarlo categoría especial de datos. No así, el tratamiento de información biométrica orientado a perfilar al alumno, siempre y cuando se pueda desvincular del primero.

Analizando la Listas de Tipos de Tratamientos de Datos que Requieren Evaluación de Impacto Relativa a Protección de Datos (Art 35.4) publicado por la AEPD, los tratamientos propuesto podrían estar dentro de los siguientes criterios, en mayor o en menor medida, para determinar que son de alto riesgo:

- Criterio 1: Tratamientos que impliquen perfilado o valoración de sujetos, incluida la recogida de datos del sujeto en múltiples ámbitos de su vida (desempeño en el trabajo, personalidad y comportamiento), que cubran varios aspectos de su personalidad o sobre sobre sus hábitos.
- Criterio 2: Tratamientos que impliquen la toma de decisiones automatizadas o que contribuyan en gran medida a la toma de tales decisiones, incluyendo cualquier tipo de decisión que impida a un interesado

el ejercicio de un derecho o el acceso a un bien o un servicio o formar parte de un contrato.

- Criterio 4: Tratamientos que impliquen el uso de categorías especiales de datos a las que se refiere el artículo 9.1 del RGPD, datos relativos a condenas o infracciones penales a los que se refiere el artículo 10 del RGPD o datos que permitan determinar la situación financiera o de solvencia patrimonial o deducir información sobre las personas relacionada con categorías especiales de datos.

- Criterio 5: Tratamientos que impliquen el uso de datos biométricos con el propósito de identificar de manera única a una persona física

- Criterio 10: Tratamientos que impliquen la utilización de nuevas tecnologías o un uso innovador de tecnologías consolidadas, incluyendo la utilización de tecnologías a una nueva escala, con un nuevo objetivo o combinadas con otras, de forma que suponga nuevas formas de recogida y utilización de datos con riesgo para los derechos y libertades de las personas.

Por lo tanto, en un primer análisis son tratamientos de alto riesgo.

Identificación por reconocimiento biométrico del alumno

La identificación por reconocimiento biométrico resulta en el tratamiento de una categoría especial de datos.

Si llevamos a cabo una evaluación inicial del tratamiento con el fin de definir el potencial alcance del impacto sobre el interesado podríamos decir que, incluso con la única finalidad de identificación el impacto sobre el interesado tiene un potencial de riesgo muy alto. Esta afirmación es posible teniendo en cuenta, además del análisis realizado en el apartado anterior, por la sensibilidad de los datos y otros potenciales atributos del tratamiento como son el posible volumen de datos sobre un mismo interesado que pudiera estar siendo recopilado durante el ciclo de vida del tratamiento, el número de interesados sobre los que se aplicaría y la exactitud de los datos teniendo en cuenta las consecuencias de los posibles falsos positivos/negativos sobre los interesados.

Por otro lado, no se justifica la necesidad del tratamiento, ya que la identificación online de los alumnos ya se ha estado realizando de forma habitual mediante la visualización del alumno, su seguimiento durante el periodo de formación y la muestra de la documentación incluso en la enseñanza reglada universitaria.

En cuanto a los posibles beneficios para el interesado, no puede decirse que exista un equilibro entre los posibles riesgos para el interesado y los beneficios de evitar un desplazamiento para la realización presencial de las pruebas de evaluación, salvo en supuestos excepcionales como el ocasionado por la pandemia, en el que deberían valorarse atendiendo a las indicaciones de las autoridades sanitarias.

Finalmente, el responsable deberá demostrar que el volumen de datos biométricos capturado de un mismo interesado es el mínimo necesario para la finalidad que se persigue en el caso de que no sólo se realice reconocimiento facial, sino tratamientos biométricos añadidos como la huella dactilar, su forma de teclear, y de la forma en la que utiliza el ratón.

Tratamiento biométricos para perfilado

Un tratamiento adicional propone el análisis de patrones biométricos, fundamentalmente mediante reconocimiento facial, pero en su caso utilizando otras fuentes de información biométrica para, entre otros, analizar que:

- El estudiante no se ha desplazado o abandonado su sitio frente al terminal durante el periodo asignado a la realización de la prueba.
- No ha sido sustituida por persona distinta
- Tiene otro comportamiento clasificado como anómalo basados en las expresiones corporales del alumno como, por ejemplo, su expresión facial, los movimientos del ratón o la forma de teclear con el objetivo de generar un patrón único para cada alumno

Tras dicho análisis, este tipo de aplicaciones generan un informe por alumno, clasificándolos en función del riesgo a que hayan infringido alguna norma del examen basándose en un algoritmo de inteligencia artificial. Dicho riesgo o alerta, se dirige al profesor para revisar de forma selectiva las grabaciones de determinados alumnos.

Aunque se puede aducir que no existe decisión automatizada, en la medida que la alerta enviada al profesor de que existe una posible infracción implica que el profesor realiza la revisión, hay una decisión automatizada en el sentido contrario: el sistema selecciona aquellos alumnos cuyo proceso de evaluación (en cuanto a la posibilidad de fraude) no van a ser revisados.

Si todas las grabaciones son revisadas en tiempo real o diferido por el profesor, no existe necesidad del tratamiento biométrico.

Por consiguiente, las garantías a adoptar serán las que resulten del correspondiente análisis de riesgos y de la evaluación de impacto y que deberá valorar el responsable del tratamiento, en el presente caso, la universidad que pretenda implantarlo. **Además, deberá consultar a la autoridad de protección de datos competente antes de proceder al tratamiento cuando la evaluación de impacto muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para mitigarlo (artículo 36), salvo que el responsable sea capaz de garantizar que el riesgo puede mitigarse por medios razonables en cuanto a tecnología disponible y costes de aplicación (Considerando 94 del RGPD).**

Y, en el supuesto más frecuente de que el tratamiento se vaya a realizar por un **encargado del tratamiento**, deberá seleccionarse uno que ofrezca garantías suficientes y haberse suscrito un contrato con el contenido del artículo 28 RGPD, en el que deberá quedar plenamente garantizado que el encargado actuará solo siguiendo instrucciones del responsable, debiendo dichas instrucciones contemplar todas las garantías adecuadas.

Asimismo, deberán adoptarse las **medidas de seguridad** necesarias conforme a lo previsto en el artículo 32 del RGPD, teniendo en cuenta, en

relación a lo consultado respecto del Esquema Nacional de Seguridad, aplicable sólo a las universidades públicas, que las medidas a adoptar no serían solo las de dicho Esquema, sino las que resulten del correspondiente análisis de riesgos. En este sentido, en el Informe de esta Agencia 170/2018, de 12 de noviembre de 2018, relativo a la compatibilidad funcional del delegado de protección de datos del RGPD y el responsable de seguridad del Esquema Nacional de Seguridad, se señalaba lo siguiente:

> "Por lo tanto, no cabe duda de que la garantía de la seguridad de los datos personales adquiere una especial trascendencia en cuanto a su protección, pero sin que ésta se limite exclusivamente al ámbito de la seguridad de dicha información, en cuanto que la protección de datos personales tiene un ámbito mucho más extenso que abarca, como decíamos, a un conjunto de principios, derechos y obligaciones mucho más amplio".

Y tal y como ha venido informando reiteradamente esta Agencia al analizar las políticas de seguridad de la información de los diferentes ministerios, en el caso de que las medidas a implantar como consecuencia del análisis de riesgos previsto en la normativa sobre protección de datos personales, en caso de resultar agravadas respecto de las previstas en el Esquema Nacional de Seguridad deberían prevalecer sobre éstas últimas, a fin de dar adecuado cumplimiento a lo exigido por dicha normativa.

Por último, y sin perjuicio del resultado del análisis de riesgos y de la evaluación de impacto y de las medidas de garantía que se adopten, así como del análisis que pueda realizar esta Agencia en el supuesto de que se le formule la consulta previa anteriormente referida, debe adelantarse que el criterio de la misma, en relación al tratamiento de datos biométricos, considera más garantista que el dato biométrico permanezca en poder del afectado.

En este sentido, ya se pronunciaba el informe 65/2015:

> Y es en este punto donde nuevamente debe traerse a colación todo lo que se ha venido indicando en relación con la especial naturaleza que a los datos biométricos va a conferir en el futuro el derecho de la Unión Europea y que exige una especial atención no sólo a la proporcionalidad sino a la propia minimización del dato; es decir, que el dato sólo sea objeto de tratamiento en tanto éste resulte completamente imprescindible para el cumplimiento de la finalidad perseguida. Ciertamente, el sistema descrito implica la adopción de medidas reforzadas para garantizar la confidencialidad de los datos, tales como la conversión de la huella a su algoritmo, el cifrado de la información, la vinculación a un dato distinto de la identificación directa del alumno o la limitación de los protocolos de acceso a los datos. Sin embargo, cabría plantearse si no sería aún posible una menor injerencia en el derecho

fundamental a la protección de datos de los alumnos que se produce como consecuencia del hecho de que el algoritmo de su huella digital se incorpora al sistema, permaneciendo en el mismo en tanto el alumno sea usuario del comedor del centro consultante, dado que en caso contrario no sería posible la verificación en tiempo real del uso de esas instalaciones. A nuestro juicio este objetivo podría lograrse si se estableciese un sistema de control del acceso al comedor que, sin perjuicio de aplicar medidas de control biométrico, permitiera que el propio dato biométrico, la huella dactilar del alumno, permaneciese bajo el control de aquél y no fuera incorporado al sistema. De este modo, sería posible que la verificación se llevase a cabo a partir de un dispositivo que portase el propio alumno, de forma que el sistema únicamente almacenase la información referida al uso o no uso del comedor, sin que en ningún momento reflejase el algoritmo de la huella. Así, sería posible que la información que según el sistema descrito sería recogida y almacenada en el propio sistema se incorporase a una tarjeta inteligente en poder del alumno que, para acceder a las instalaciones, hubiese de utilizar la tarjeta y al propio tiempo posicionar su huella sobre el lector. De este modo, en caso de que el algoritmo resultante del posicionamiento fuera coincidente con el que contuviera la tarjeta sería posible el acceso, no admitiéndose el mismo en caso de no producirse la citada coincidencia. El sistema así únicamente almacenaría la información identificativa del alumno y en ningún caso incluiría la relacionada con el algoritmo de la huella dactilar, lo que minimizaría la injerencia de la medida adoptada sin por ello perjudicar el resultado que la misma pretende conseguir, en los términos que se describen en la consulta.

En consecuencia, esta Agencia considera que sólo sería ajustado al principio de proporcionalidad un sistema de reconocimiento dactilar que, por una parte, y como en el supuesto planteado, quede reducido a determinadas dependencias del centro, particularmente el comedor y, por otra permita que los medios de verificación, en este caso el algoritmo de la huella dactilar del alumno, permanezcan en su poder y no sean incorporados al sistema, que sólo incluiría los datos referentes a la identificación del alumno que accede al comedor, al producirse una verificación positiva del mismo.

Por todo ello, y según lo establecido en el artículo 25 del RGPD con relación a la aplicación de medidas de privacidad desde el diseño y por defecto, para disminuir el riesgo del tratamiento es recomendable que sea el interesado quien mantenga el máximo control sobre sus datos, en particular sobre los datos biométricos. La implementación del principio de control del usuario incluye, entre otros, el almacenamiento de dichos datos en dispositivos bajo su custodia y que incorporen las necesarias garantías para que el acceso a dicha información no esté comprometido.

VII

Para concluir, se recuerda que, tal y como se indicaba al principio del presente informe, el mismo se centra en el análisis jurídico de las cuestiones planteadas en la consulta referidas al uso de técnicas de reconocimiento facial en la realización de pruebas de evaluación online.

Por consiguiente, aunque se han hecho referencia a las mismas, no son objeto de estudio el resto de medidas que se pueden adoptar por las universidades para la realización de las evaluaciones online, teniendo en cuenta que la propia consultante, en su "Informe sobre Procedimientos de Evaluación no Presencial. Estudio del Impacto de su Implantación en las Universidades Españolas y Recomendaciones" de 16 de abril de 2020 (http://www.crue.org/Documentos%20compartidos/Informes%20y%20Posicionamientos/Informe%20procedimientos%20evaluacion%20no%20presencial.pdf), identifica **11 procedimientos de evaluación no presencial diferentes**, en los que se pueden adoptar diferentes medidas al objeto de garantizar la identidad de los alumnos y la autoría de las actividades. No obstante, **todas las medidas que puedan adoptarse deberán respetar, igualmente, lo establecido en la normativa de protección de datos personales.**

Por otro lado, hay que tener en cuenta que en la práctica se pueden aplicar conjuntamente diferentes medidas y sistemas, lo que puede suponer una intromisión aún mayor en el derecho a la protección de datos personales de los alumnos. En estos casos, **deberá evaluarse conjuntamente todas las medidas que se pueden implantar y su conformidad con el RGPD, atendiendo a los diferentes principios de protección de datos y, singularmente, al de minimización de datos, de modo que solo se traten los datos estrictamente necesarios para la finalidad pretendida**. Esto supone que, una medida que, aisladamente considerada, pueda ser conforme al RGPD, en su combinación con otras pueda dar lugar a que el tratamiento de datos sea excesivo. Asimismo, hay que tener en cuenta que hay medidas que ya, por sí solas, implicarían un tratamiento excesivo para la finalidad pretendida por la universidad, como puede ser el análisis biométrico de las pulsaciones sobre el teclado, más aún cuando se combinan con otras como el reconocimiento facial.

Por último, hay que indicar que, como recuerda el Grupo del 29 en su Dictamen 2/2013 sobre las aplicaciones de los dispositivos inteligentes, **en el caso de que la tecnología empleada implique el almacenamiento de la información o la obtención del acceso a información ya almacenada en el dispositivo de los alumnos por la universidad o el encargado del tratamiento**, resultaría de aplicación el artículo 5.3 de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el

sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas), transpuesta a nuestro ordenamiento jurídico por el artículo 22.2 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, en la redacción dada por la disposición final quinta de la ley 9/2014, de 9 de mayo, General de Telecomunicaciones, por lo que dicho acceso **requeriría, independientemente de la base jurídica que legitime el tratamiento conforme al RGPD, el consentimiento del alumno:**

> 2. Los prestadores de servicios podrán utilizar dispositivos de almacenamiento y recuperación de datos en equipos terminales de los destinatarios, a condición de que los mismos hayan dado su consentimiento después de que se les haya facilitado información clara y completa sobre su utilización, en particular, sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
>
> Cuando sea técnicamente posible y eficaz, el consentimiento del destinatario para aceptar el tratamiento de los datos podrá facilitarse mediante el uso de los parámetros adecuados del navegador o de otras aplicaciones.
>
> Lo anterior no impedirá el posible almacenamiento o acceso de índole técnica al solo fin de efectuar la transmisión de una comunicación por una red de comunicaciones electrónicas o, en la medida que resulte estrictamente necesario, para la prestación de un servicio de la sociedad de la información expresamente solicitado por el destinatario.