https://doi.org/10.1344/REYD2020.22.32357

# *Tecnología de verificación de identidad y control en exámenes online.*

## *Facial Recognition identity verification an control of Online Exams*



**Ricard Martínez Martínez**

Profesor contratado-doctor de Derecho Constitucional.
Director de la Cátedra de privacidad y Transformación Digital Microsoft-Universitat de Valencia.
Derecho Constitucional, Ciencia Política y de la Administración de la Universitat de València.
E-mail: ricard.martinez@uv.es

**Resumen:** Las tecnologías de reconocimiento facial para la verificación de identidad y de control del acceso al espacio virtual para el desarrollo de exámenes inciden muy directamente sobre los derechos del estudiante. Su implementación y uso, implica un tratamiento de datos biométricos particularmente exigido en términos de cumplimiento normativo por el Reglamento General de Protección de Datos. En ambos casos, es necesario asegurar el debido equilibrio entre los derechos del estudiante y la garantía del derecho de la institución universitaria de articular procesos de verificación de los conocimientos que eviten el fraude.

**Palabras clave:** protección de datos, Reglamento General de Protección de Datos, RGPD, reconocimiento facial, datos biométricos.

**Abstract:** Facial recognition technologies for identity verification and access control to the virtual space for the performance of exams have a strong impact on student rights. Their implementation and use, implies a biometric data processing particularly enforced in terms of regulatory compliance by the General Data Protection Regulation. In both cases, it is necessary to ensure the due balance between the rights of the student and the

guarantee of the right of the academic institutions to implement a knowledge verification procedure that prevents fraud.

**Keywords**: data protection, General Data Protection Regulation, GDPR, facial recognition, biometric data.

## 1.-Una aproximación a los hechos



Al finalizar la lectura de este trabajo es posible que el lector deba enfrentarse a una extraña sensación de melancolía. Casi antes de iniciar su redacción, el autor está en condiciones de asegurar que, salvo una acción decidida del legislador nacional, la utilización de tecnologías de reconocimiento facial con fines de verificación de identidad, control o análisis del desempeño durante una prueba de examen online, está condenada a un probable fracaso. Sin embargo, es muy posible, que el conjunto de cuestiones que suscitará nuestra aproximación a este tipo de tratamientos de información personal resulte de interés. Esto es así, en la medida en la que define retos tecnológicos de futuro que enfrenta la Universidad y, por extensión, el conjunto del sistema educativo.

La razón que alienta este planteamiento inicial se basa en una suerte de pesimismo bien informado. La implementación de sistemas de *proctoring*, cuando incorporan técnicas de reconocimiento facial mediante herramientas biométricas, se enfrenta a un rechazo de la autoridad de protección de datos que podría calificarse de genético. Efectivamente se encuentra en su ADN el rechazo de cualquier tecnología que resulte invasiva respecto del derecho fundamental a la protección de datos. Es una posición sin duda lógica y compartida en la mayor parte de los casos. Sin embargo, resulta indispensable tener en cuenta ciertas consideraciones de hecho, que suelen resultar ajenas a los posicionamientos de estas autoridades en sus informes, guías, procedimientos sancionadores o normas interpretativas de carácter reglamentario. Debe subrayarse que este arsenal se despliega en un escenario en el que la posición jurídica del regulador resulta prácticamente invulnerable. Y si bien, ello puede resultar instrumental para la garantía de nuestro sistema de libertades en un proceso de transformación digital cuyas consecuencias podrían ser incalculables, no es menos cierto que también puede conducir

a posicionamientos radicalmente restrictivos que podrían generar disfunciones en el funcionamiento de nuestra sociedad[1].

Precisamente el primero de los objetivos de este trabajo consiste en identificar el conjunto de circunstancias conducen a las universidades a buscar soluciones de control ordenadas a evitar el fraude, la suplantación de identidad, y las conductas indebidas o deshonestas durante el desarrollo de las pruebas de verificación de los conocimientos y capacidades de las y los estudiantes. En este sentido, resulta significativo, por ejemplo, el desconocimiento de la Agencia Española de Protección de Datos sobre la realidad material de la universidad, con toda probabilidad debido a la carencia de calidad de las consultas que eventualmente se le hayan planteado. Sin embargo, esta no es excusa suficiente, tal vez el regulador debiera, llegado el caso, requerir la colaboración de interlocutores universitarios que tuvieran la capacidad de describir con detalle el objeto de una consulta cuando ésta resulta complicada.



Por ejemplo, como más adelante se examina, cuando la Agencia manifiesta su completa oposición a la utilización de sistemas de videovigilancia durante la realización de exámenes presenciales desconoce sin duda la realidad de los hechos que sin duda motivan la consulta. A día de hoy la institución universitaria se enfrenta a muy diversos supuestos en los que el estudiante deshonesto recurre a prácticas particularmente sofisticadas para copiar. Aquel estudiante que recurría a la "chuleta", el "cambiazo", o a mirar por encima del hombro convive con prácticas más sofisticadas. Hoy la suplantación de identidad en un examen se negocia en Twitter o Facebook mediante el recurso a los llamados *"informers"* e incluso directamente en páginas de anuncios[2], y prolifera un próspero negocio de venta de trabajos[3]. Del mismo modo, la Universidad

[1] Véase por ejemplo la Guía de la Agencia Española de Protección de Datos sobre el uso de las tecnologías en la lucha contra el COVID19. Podrá el lector encontrar una completa descripción de todos los inconvenientes, riesgos y peligros de la tecnología. No espere, sin embargo, ni una sola recomendación útil, ni una sola propuesta para la acción, que le permita gobernar el riesgo e implementar soluciones tecnológicas viables a los ojos del regulador. Este documento se encuentra disponible (30/09/2020) en https://www.aepd.es/es/guias-y-herramientas/guias. El autor ha opinado con cierta dureza sobre este enfoque del regulador en el Diario Cinco días. MARTÍNEZ MARTÍNEZ, R (2020). Autoridades independientes, no irresponsables, en el País-Cinco Días. Disponible (30/09/2020) en https://cincodias.elpais.com/cincodias/2020/05/25/legal/1590385284_647173.html.

[2] Véase el titular del diario Granada HOY: «200 euros por un examen de ingeniería: el fraude en las evaluaciones online de la UGR». Disponible (29/09/2020) en https://www.granadahoy.com/granada/examen-fraude-evaluaciones-online-UGR_0_1472253316.html.

[3] Un tercero opera como intermediario poniendo en contacto a sujetos que ofertan el pago por la realización del examen, o por la redacción del trabajo final de grado o final de máster, con proveedores dispuestos a cooperar en este tipo de comportamiento deshonesto. Véase SUREDA NEGRE, y COMAS FORGAS, R. (2020). La promoción del fraude académico a través de los buscadores. *The Conversation*. Disponible (29/09/2020) en https://theconversation.com/la-promocion-del-fraude-academico-a-traves-de-los-buscadores-141593

tenido la oportunidad de comprobar el recurso a herramientas tecnológicas para conectar estudiantes con personas situadas en el exterior del aula[4].

En este sentido, el único método viable para impedir estas prácticas obligaría prácticamente a un registro corporal. Precisamente por ello, si bien, puede compartirse la oposición de la AEPD al uso de videovigilancia en las aulas es evidente que no ha contemplado los hechos que motivan este tipo de consulta. La Universidad no sólo carece de competencias para desarrollar un registro corporal, a todas luces manifiestamente desproporcionado, sino que tampoco puede utilizar inhibidores en los sistemas de comunicaciones si evaluar el para la seguridad de las personas en el área inmediata al impedir, por ejemplo, las llamadas a un número de emergencia. Por otra parte, resultan evidentes las limitadas capacidades físicas de un único profesor desarrollando tareas de control de un aula para detectar este tipo de técnicas de fraude.



No discutimos, y así se ha manifestado en el informe del grupo de trabajo de la Conferencia de Rectores de las Universidades Españolas (CRUE), sobre la posibilidad de desarrollar técnicas específicas de examen que traten de evitar al máximo el fraude[5]. Lo que aquí se cuestiona, es el hecho, de que se fijen criterios por parte de un regulador con un manifiesto desconocimiento de la realidad subyacente que tal vez hubieran sido parcialmente diferentes de haberse contemplado la realidad material.

En este sentido, la situación que debían enfrentar las universidades con motivo del cese de la actividad presencial en el segundo semestre del curso 2019-2020, implicaba el riesgo de que el desarrollo de pruebas online pudiera facilitar las prácticas fraudulentas. En este sentido, es evidente la mayor probabilidad de suplantaciones de identidad en el

[4] La extrema desfachatez lleva a la comercialización sin tapujos en Amazon del producto «Pinga Vip Pro Oculto Para Exámenes (Carne)». Y con valoraciones de sus usuarios ciertamente impagables:
- El pinganillo está muy bien, es pequeño y discreto, muy difícil de ver, y se escucha perfectamente. Como receptor lleva un cable que puedes poner alrededor del cuello y, con una camisa o un polo, tampoco se ve, aunque con una camiseta puede que sí. Yo lo he usado conectado a un MP3 y el funcionamiento ha sido perfecto. Como única pega, y motivo por el cual no le doy 5 estrellas, diría que el proceso de cambiar la pila, dado su pequeño tamaño, es un poco delicado y, si no tienes cuidado, puedes romper el pinganillo. Teniendo esto en cuenta y haciendo el cambio con el debido cuidado, no tiene por qué romperse.
- **Se olle** muy bien, un pequeño ruido de fondo, pero se escucha perfectamente, cuanto más cerca este el cable trasmisor mejor se oye.
Disponible (29/09/2020) en https://www.amazon.es/product-reviews/B077M8LCLH/ref=acr_dpx_hist_5?ie=UTF8&filterByStar=five_star&reviewerType=all_reviews#reviews-filter-bar.
N. del A.-Es nuestra la negrita subrayando la falta de ortografía que, obviamente, acreditan las razones del estudiante para acudir a estos medios.

[5] Informe del Grupo de Trabajo Intersectorial de Crue Universidades sobre Procedimientos de Evaluación no Presencial. Estudio del Impacto de su Implantación en las Universidades Españolas y Recomendaciones Españolas, Versión 1.0 de jueves 16 de abril de 2020. Disponible (30/09/2020) https://www.crue.org/informes-y-posicionamientos/

desarrollo de pruebas online. Y no sólo se trata de prever, y evitar estas suplantaciones, existían otras prácticas a prevenir como la realización de exámenes colectivos o compartidos a través de sistemas de mensajería. Así como de cualquier otro medio a través del uso de herramientas como buscadores, textos previamente redactados, y cualesquiera otros que la imaginación humana pueda alumbrar.

Por ello en un contexto que multiplica exponencialmente los riesgos de fraude en entornos online un análisis jurídico que sitúa en el centro de modo absoluto y prevalente el derecho fundamental a la protección de datos puede resultar cuando menos limitado. En la aproximación de la AEPD, que se examinará en profundidad, cuenta exclusivamente la relación entre las técnicas de verificación empleadas, y el derecho fundamental a la protección de datos. En ausencia de norma, predeterminación normativa no existe solución viable.



Sin embargo, no se tiene en cuenta en absoluto el impacto social de tales prácticas. En el llamado "sistema de Bolonia", implantado con mejor o peor fortuna en España, se supone que el conjunto de técnicas de evaluación conduce a la verificación de competencias y conocimientos. El resultado último comporta la certificación por parte de la institución universitaria de que tales capacidades, conocimientos y competencias se han alcanzado. En muchos ámbitos profesionales esta certificación habilita al egresado para el desempeño profesional directo e inmediato. En consecuencia, la carencia de control del fraude en el desempeño de las pruebas de evaluación universitaria, no sólo pone en riesgo a la propia institución, sino que se proyecta sobre la sociedad entera que acoge en su seno a egresados cuya conducta ética es cuestionable y cuya capacitación se ha falseado. Esta dimensión comunitaria de los derechos, esta consideración de los conflictos de hecho desde el punto de vista de los deberes éticos y jurídicos del estudiante, es ajena a cualquier análisis realizado por las autoridades de protección de datos. Y eso supone, con toda seguridad un riesgo evidente a la hora de definir una respuesta jurídica adecuada capaz de conciliar todos los intereses en presencia. Y en este sentido, y sin perjuicio de las conclusiones finales de esta publicación, es necesario subrayar la constante y manifiesta tendencia del regulador a convertir el derecho fundamental a la protección de datos en un derecho de carácter preferente que se impone en cualquier relación jurídica que se someta a su consideración, cediendo o modulándose en muy escasas ocasiones. Esta puede ser una buena noticia desde la perspectiva de una concepción individualista de los derechos fundamentales, y desde la plena seguridad en que el derecho fundamental a la protección

datos siempre será tutelado. Pero no es la menor la mejor de las noticias cuando se trata de defender una interpretación sistemática del ordenamiento, una aproximación a los conflictos de derechos desde la ponderación de bienes y valores constitucionales, o de la búsqueda de soluciones equilibradas y viables.

### 1.2 Modalidades de examen online.

El Grupo de Trabajo Intersectorial de Crue (2020)[6], al que se encomendó identificó once técnicas posibles para el desarrollo de pruebas de evaluación. El objetivo de esta categorización no era otro que el de establecer posibles metodologías de verificación de conocimientos funcionales a un entorno de evaluación 100% online. Los tipos de evaluación identificados y clasificados son los que siguen:



1. Examen oral.
2. Prueba escrita abierta.
3. Prueba objetiva.
4. One minute paper.
5. Trabajo académico.
6. Mapas conceptuales.

[6] Este Grupo estuvo integrado por representantes de CRUE Docencia, CRUE Secretarías Generales, CRUE TIC y CRUE Asuntos Estudiantiles.

- *Oscar Cordón*. **Coordinador**. Miembro de la Ejecutiva de CRUE TIC y Presidente del GT sobre Formación Online y Tecnologías Educativas (FOLTE). Universidad de Granada.
- *Ángela Alcalá*. Secretaria Ejecutiva de CRUE Asuntos Estudiantiles. Vicerrectora de Estudiantes y Empleo de la Universidad de Zaragoza.
- *Mónica Arenas*. Miembro del GT de Delegados de Protección de Datos (DPDs) de CRUE Secretarías Generales. Delegada de Protección de Datos de la Universidad de Alcalá.
- *Juan Camarillo*. Miembro de la Ejecutiva de CRUE TIC y del GT FOLTE. Director para la Universidad Digital de la Universidad de Sevilla.
- *Dulce Mª García*. Miembro de la Ejecutiva de CRUE Secretarías Generales y Presidenta del GT de DPDs. Secretaria General de la Universidade de Santiago de Compostela.
- *José Pascual Gumbau*. Miembro del GT de DPDs de CRUE Secretarías Generales. Delegado de Protección de Datos de la Universitat Jaume I.
- *Juan Manuel Martín*. Miembro de la Ejecutiva de CRUE Docencia y Vicerrector de Docencia de la Universidad de Granada.
- *Ricard Martínez*. Miembro del GT de DPDs de CRUE Secretarías Generales. Delegado de Protección de Datos de la Universidad de Valladolid, Universidad de Burgos, Universidad de Salamanca, Universidad de La Laguna y Universitat Politècnica de València. Profesor de Derecho Constitucional en la Universitat de Valencia.
- *Mercè Puig*, Vicerrectora de Estudiantes y Política Lingüística de la Universitat de Barcelona.
- *Francisco Sampalo*. Miembro de la Ejecutiva de CRUE TIC y Presidente del GT sobre Seguridad y Auditoría TI. Responsable de Seguridad de la Información de la Universidad Politécnica de Cartagena.
- *Eduardo Vendrell*. Miembro de la Ejecutiva de CRUE Docencia y Vicerrector de Estudios, Calidad y Acreditación de la Universitat Politècnica de València.

7. Diario reflexivo.

8. Portafolio.

9. Observación.

10. Proyectos.

11. Problemas/Casos.

A su vez, tales pruebas eran susceptibles de ser realizadas a través de tres entornos o canales distintos.

1. Aula virtual.

2. Canales de videoconferencia.

3.-Entornos de trabajo en cloud.

Asimismo, para la ejecución de las pruebas los delegados de protección de datos identificaron los potenciales tratamientos de datos personales necesarios en todos los escenarios o canales descritos. Todos ellos cumplían con ciertas finalidades comunes:



1. Identificación de las personas evaluadas y de los evaluadores.

2. Gestión administrativa y académica de las pruebas.

3. Controles sobre el normal desarrollo de la prueba y garantía de las exigencias de transparencia y seguridad jurídica de los procesos de evaluación.

4. Corrección de las pruebas.

5.-Procesos de revisión ordinaria o primera revisión de las pruebas.

Desde el punto de vista de este artículo, el uso de datos de identificación integra dos tipos de procedimiento considerados viables:

1. Uso de claves concertadas en el acceso a los sistemas de información.

2. Verificación visual de la identidad de los estudiantes y de sus acciones durante la prueba.

En los distintos tipos de canales existían tratamientos específicos que se sumaban a los usuales:

| Canal | Titularidad | Tipo | Tratamiento |
|---|---|---|---|
| | | | Común: identificación<br>Seguimiento mediante webcam |
| **Aula virtual** | Propia<br>(puede existir un proveedor de servicios de alojamiento)<br>Integra o usa herramientas antiplagio ajenas | 2. Prueba escrita abierta. | |
| | | 3. Prueba objetiva. | |
| | | 4. One minute paper. | |
| | | 5. Trabajo académico. | Datos incorporados a las tareas: entrevistas, grabaciones, videos, fotografías. |
| | | 6. Mapas conceptuales. | |
| | | 7. Diario reflexivo. | Datos subjetivos o de personalidad |
| | | 8. Portafolio. | Datos incorporados a las tareas: entrevistas, grabaciones, videos, fotografías |
| | | 10. Proyectos. | Datos incorporados a las tareas: entrevistas, grabaciones, videos, fotografías |
| | | 11. Problemas/Casos. | Seguimiento mediante webcam<br>Grabaciones |
| **Videoconferencia** | Proveedor de servicios | 1. Examen oral. | |
| | | 2. Prueba escrita abierta. | Seguimiento mediante webcam<br>Grabaciones |
| | | 3. Prueba objetiva. | |
| | | 9. Observación. | Seguimiento mediante webcam<br>Grabaciones |
| | | 9. Observación. | |
| **Entornos de trabajo en cloud** | Proveedor de servicios | 4. One minute paper. | |
| | | 6. Mapas conceptuales. | Datos incorporados a las tareas: entrevistas, grabaciones, videos, fotografías |

**Fig.1 Fuente Informe sobre el impacto normativo de los procedimientos de evaluación online: protección de datos y garantía de los derechos de las y los estudiantes.**

Adicionalmente se consideraron las finalidades, tipos de datos en relación con determinados tratamientos especialmente cualificados en función del tipo de prueba.

| Prueba | Finalidad | Datos | Tratamiento |
|---|---|---|---|
| Común | Controlar actuaciones arbitrarias o ilícitas | Con carácter común: profesor responsable, identificación del estudiante que se examina | Depende de cada prueba |
| 1. Examen oral. | Registro de la prueba | Imagen y voz | Grabación |
| 2. Prueba escrita abierta. | Antiplagio | Datos de estudiantes plagiados | Analítica de datos |
| 3. Prueba objetiva. | Antiplagio | Datos de estudiantes plagiados | Analítica de datos |
| 4. One minute paper. | Antiplagio | Datos de estudiantes plagiados | Analítica de datos |
| 5. Trabajo académico. | Antiplagio | Datos de estudiantes plagiados | Analítica de datos |
| 6. Mapas conceptuales. | Antiplagio | Datos de estudiantes plagiados | Analítica de datos |
| 7. Diario reflexivo. | Antiplagio | Datos de estudiantes plagiados | Analítica de datos |
| 8. Portafolio. | Antiplagio | Imagen y voz<br><br>Datos de personas participantes | Grabación |
| 9. Observación. | Registro de la prueba | Imagen y voz | Grabación |
| 10. Proyectos. | Antiplagio | Imagen y voz<br><br>Datos de personas participantes | Grabación |
| 11. Problemas/Casos. | Antiplagio | Datos de estudiantes plagiados | Analítica de datos |

**Fig.2 Fuente Informe sobre el impacto normativo de los procedimientos de evaluación online: protección de datos y garantía de los derechos de las y los estudiantes.**

El citado Informe sobre el impacto normativo de los procedimientos de evaluación online rechazó de raíz el empleo de técnicas de reconocimiento facial como metodología de verificación de la identidad y control en la realización de exámenes online. La razón para ello no era otra que el riesgo regulador. En este sentido merece la pena reproducir íntegramente las consideraciones del documento:

> «El subgrupo de trabajo, integrado por delegados de protección de datos de las universidades, ha considerado excluir de estas recomendaciones las técnicas de reconocimiento facial (sistemas de proctoring). Debido a la 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.
>
> • Considerar las condiciones de regulación que ofrezcan una adecuada seguridad jurídica.»[7]



De la descripción precedente, resulta evidente la extraordinaria complejidad que plantea la gestión jurídica del desarrollo de una prueba online. Así mismo, debe destacarse cómo los delegados de protección de datos descartaron de raíz el uso de técnicas de reconocimiento facial. Se examinan a continuación las razones para ello.

### 1.3 Una tecnología no exenta de riesgos.

Finalmente, desde el punto de vista de los hechos resulta imprescindible señalar que las autoridades de protección de datos han definido un escenario de riesgos y vulnerabilidades. De entre ellas, subrayaremos las aportaciones de la CNIL[8] y de la AEPD junto al EDPS[9]. Así, la autoridad francesa, señala que el reconocimiento facial puede cumplir dos funciones distintas:

▪ La autenticación de una persona, que tiene por objeto verificar que una persona es quien dice ser. En este caso, el sistema comparará una plantilla biométrica prerregistrada (por ejemplo, almacenada en una tarjeta inteligente) con una sola cara.

▪ La identificación de una persona, que tiene por objeto encontrar a una persona dentro de un grupo de individuos, en un lugar, una imagen o una base de datos. En este caso, el sistema

---

[7] MARTÍNEZ MARTÍNEZ, R., ARENAS RAMIRO, M, y PASCUAL GUMBAU, J. (2020) Informe sobre el impacto normativo de los procedimientos de evaluación online: protección de datos y garantía de los derechos de las y los estudiantes. Madrid, CRUE, pág. 26. Disponible (30/09/2020) en https://www.usal.es/files/wp_cumplimiento.eval_.pdp_-_rm-ma-jpg.final-2020.04.15.pdf.pdf

[8] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS-CNIL (2109). *Reconnaissance faciale: pour un débat à la hauteur des enjeux*. Disponible (30/09/2020) en https://www.cnil.fr/fr/reconnaissance-faciale-pour-un-debat-la-hauteur-des-enjeux

[9] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS-AEPD y EUROPEAN DATA PROTECTION SUPERVISOR-EDPS (2020). *14 equívocos con relación a la identificación y autenticación biométrica*. Disponible (30/09/2020) en https://www.aepd.es/es/guias-y-herramientas/guias.

debe realizar una prueba en cada cara capturada para generar una plantilla biométrica y verificar si corresponde a una persona conocida por el sistema. Esta funcionalidad se basa, por lo tanto, en la comparación de una plantilla con una base de datos de plantillas.

El potencial de las tecnologías de identificación ofrece numerosas y más diversas aplicaciones que identifica el regulador francés:

▪ Reconocimiento automático de las personas presentes en una imagen con el fin de identificar, por ejemplo, sus relaciones en una red social.

▪ Acceso a s servicios, como cajeros automáticos.

▪ Trazar un pasajero de un servicio de transporte en todas las etapas del viaje o reconstruir el viaje de una persona y sus sucesivas interacciones con terceros, por ejemplo para identificar sus contactos.



▪ Búsqueda policial de sujetos en una base de datos que contenga fotografías.

▪ Vigilancia de los movimientos de una persona en el espacio público o identificación en la vía pública de las personas buscadas.

Vistas las posibilidades que ofrece esta tecnología, se señala que, si bien puede haber casos legítimos y lícitos de utilización del reconocimiento facial, no deben llevar a la creencia de que todo sería deseable o posible. En cuanto a los riesgos, a partir de la consideración de los datos biométricos como categorías especiales de datos, se señalan entre otros:

▪ Los riesgos relacionados con la seguridad de la información.

▪ El fácil acceso a imágenes de las personas y la pérdida de control sobre las mismas incluso durante el proceso de captación.

▪ La posibilidad de usarlas con fines de videovigilancia general o masiva con la consiguiente pérdida de privacidad en el espacio público.

▪ La falibilidad de una tecnología no exenta de errores y sesgos en su funcionamiento.

La AEPD y el EDPS han identificado “equívocos” en relación con la identificación biométrica. Entre estos cabe destacar:

▪ A diferencia de una contraseña o un certificado, los datos biométricos recogidos durante un procedimiento de autenticación o identificación revelan más información personal sobre el sujeto.

▪ A diferencia de los procesos basados en contraseñas o certificados, que es 100% precisa la identificación/autenticación biométrica se basa en probabilidades y existe una determinada tasa de falsos positivos.

- En las condiciones medioambientales en entornos no controlados provoca el aumento de la tasa de error y por tanto que la confusión sea más probable.

- Algunas personas no pueden utilizar determinados tipos de biometría porque sus características físicas no son reconocidas por el sistema.

▪ Existen procedimientos y técnicas que permiten burlar sistemas de autenticación biométrica y asumir la identidad de otra persona.

▪ La mayor parte de características biométricas de una persona están expuestas y se pueden capturar a distancia.

▪ Cualquiera de los múltiples sistemas en los que nuestros datos biométricos estén siendo procesados puede sufrir una brecha de seguridad.



▪ Por definición, un sistema de autenticación fuerte es aquel que exige que se proporcione, al menos, dos de los siguientes: algo que se sabe, algo que se tiene o algo que se es (biometría). Por definición, sólo utilizar biometría es un proceso de autenticación débil, mientras que utilizar una tarjeta de acceso y contraseña es fuerte.

Como se apreciará con posterioridad, esta percepción del riesgo, o el equívoco modula la aproximación jurídica de la autoridad de protección de datos a la cuestión del uso del reconocimiento facial en la verificación de identidad y control de los exámenes.

## 2. El tratamiento de datos relacionados con el reconocimiento facial.

Desde el punto de vista del Reglamento General de Protección de Datos (RGPD)[10] La verificación de identidad realizada mediante técnicas de reconocimiento facial plantea la cuestión de categorizar la naturaleza de tales datos. A tal efecto, el Reglamento ofrece en su artículo 4 la definición de dato biométrico en los siguientes términos:

> 14) «datos biométricos»: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos;

Estos datos, según señala la Agencia Española de Protección de Datos en su Informe núm. 0036/2020, -al que dedicamos más adelante un epígrafe-, tendrán la consideración de categorías especiales de datos en el siguiente supuesto[11]:

[10] 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.

[11] La autoridad toma como referencia distintos documentos, cuya reproducción debe incluirse aquí habida cuenta de su interés:

> «(…) 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).

> «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).»

A criterio de la Unidad de Evaluación y Estudios Tecnológicos de la Agencia Española de Protección de Datos, los tratamientos de reconocimiento facial que sometió a su consideración la CRUE implicaba el tratamiento de datos biométricos[12]. Esto supone, cómo señalaban los delegados de protección de datos de las universidades, la necesidad de aplicar las previsiones del artículo 9 del RGPD. La norma parte, de una prohibición de uso por defecto en su párrafo primero, que sólo puede ser excepcionada por la legislación nacional o el Derecho de la Unión en los supuestos de su párrafo segundo[13].



En la práctica, el artículo 9 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales admite el tratamiento de datos biométricos

---

> 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".

[12] En este sentido señalaba:

> «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.»

La AEPD coincide expresamente en el informe de referencia con 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 cuando considera el empleo de videovigilancia con reconocimiento facial como categoría especial de datos.

[13] Esta norma dispone:

> **Artículo 9**
> **Tratamiento de categorías especiales de datos personales**
> 1. Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física.
> 2. El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes:
> 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;

con consentimiento, requiriendo el desarrollo de una norma con rango de ley cuando se invoquen como fundamento del tratamiento razones de un interés público esencial. Esto es, bien el consentimiento, bien un interés público relevante, serían los potenciales fundamentos jurídicos invocables para el uso del reconocimiento facial en la realización de exámenes online. En el momento álgido de la primera ola de la pandemia, y el contexto de una docencia impartida exclusivamente online, sólo existía una alternativa para el desarrollo de las pruebas: las herramientas virtuales de las universidades. Por tanto, no se daban en absoluto las condiciones que para un consentimiento libre vienen reclamando las autoridades de protección de datos. Así, el llamado Working Party, también conocido como GT29 o Grupo de Trabajo del artículo 29, -hoy Comité Europeo de Protección de Datos o EDPB por sus siglas en inglés-, señala que:



> 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. (…)
>
> 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.
>
> (…) Los desequilibrios de poder no se limitan a las autoridades públicas y a los empleadores, sino que también pueden producirse en otras situaciones. (…) El consentimiento no será libre en aquellos casos en los que exista un elemento de compulsión, presión o incapacidad para ejercer la libre voluntad.

### 3.1 Los precedentes en los informes de la Agencia Española de Protección de Datos

La posición del regulador, ha sido históricamente restrictiva respecto del empleo de técnicas de control invasivas en las instituciones educativas. En el Informe núm. 0392/2011, anterior a la actual regulación, aplicable desde el 2018, la AEPD se refería al tratamiento de los datos necesarios para el reconocimiento de los alumnos de un centro universitario a través de programas de reconocimiento facial para la identificación de los mismos en la realización de las correspondientes pruebas. La AEPD realizado un juicio que exige superar los principios de idoneidad, necesidad y proporcionalidad en sentido estricto o determinación de un interés público prevalente, la Autoridad se manifestó negativamente respecto del uso de esta medida al considerar que:

> la finalidad de control de asistencia podría lograrse igualmente a través de otros mecanismos, habitualmente utilizados hasta la fecha, que garanticen una mayor seguridad en el logro del objetivo sin necesidad de exigir el tratamiento del dato de la huella digital, sin que sea óbice para ello la mera afirmación de que dichos mecanismos son menos seguros que los que pretenden implantarse, por

> cuanto es posible el establecimiento de medidas más seguras de control que impidan la vulneración de los controles sin necesidad de por ello proceder al tratamiento de los datos de reconocimiento facial de los alumnos, con los consiguientes riesgos que ello pudiera aparejar.

Sin embargo, en el mismo informe, se señalaba que el juicio de ponderación resulta altamente dependiente de las condiciones concretas. Por otra parte, el Informe de la AEPD núm. 0186/2017 sobre grabación de las imágenes de los alumnos durante la realización de los exámenes en el entorno de una Universidad, señala:

> 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".
>
> (…)
>
> La instalación de cámaras en las aulas con la finalidad de disuadir a los alumnos de cometer determinadas conductas inapropiadas durante la celebración de los exámenes, sólo podría considerarse bajo determinadas circunstancias y con especiales salvaguardas, pero no como una medida a implementar con carácter general en la Universidad. Recordemos que se está planteando la captación de imágenes en el interior de un espacio semiprivado, 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.

Por último, podemos hacer referencia al extenso informe de la AEPD en relación con los tratamientos de datos efectuados en el ámbito universitario (Informe jurídico núm. 0036/2019). En él, se descarta la virtualidad del consentimiento como elemento legitimador de la publicación de las calificaciones. La asimetría en la relación jurídica entre el estudiante y la universidad es determinante para ello[14].

[14] Señala la Agencia Española de Protección de Datos:

> «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».
>
> Concluyendo que:

### 3.2 La posición de las universidades

Desde un punto de vista práctico, durante la realización de un examen, se vienen tratando distintos tipos de datos en el mundo físico. Uno de ellos 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 ser suplantado en su identidad por otra persona. Sin embargo, esta posibilidad de control y vigilancia desaparece por completo cuando se trata de realizar un examen online desde el propio domicilio. 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 usando herramientas de videoconferencia o webcams.

A estos dos 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.

En un contexto 100% online, las posibilidades que ofrecen los métodos tradicionales no resultan tan eficientes como el empleo de técnicas de reconocimiento facial. En primer lugar, la verificación de la correspondencia entre la imagen del estudiante en los registros de un aula virtual, generalmente de baja calidad, resulta visualmente dificultosa. Por otra parte, identificar una a una a todas las personas concurrentes a una prueba "pasando lista" implica un coste elevado de tiempo. Además, la exhibición en pantalla de un Documento Nacional de Identidad puede suponer una innecesaria exhibición de datos ante toda la clase. Si a ello añadimos problemas adicionales como el complejo seguimiento de una prueba remota en pantalla, resulta evidente la fragilidad y escasa operatividad del mero visionado.

---

«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.».

Desde el punto de vista del régimen jurídico aplicable en el contexto universitario, los delegados implicados en el informe arriba referido[15], elaboraron una propuesta de consulta de la Conferencia de Rectores de las Universidades Españolas a la Agencia Española de Protección de Datos que examinaba las condiciones jurídicas de legitimación de las metodologías de control de exámenes y verificación de identidad. Como es sabido, un elemento determinante en la prestación del servicio público de educación superior consiste en la verificación objetiva de los conocimientos de las y los estudiantes. El desarrollo de la actividad de evaluación se configura en nuestro Ordenamiento como una actividad de naturaleza compleja. En primer lugar, la verificación de los conocimientos del estudiantado es una facultad, que integra la autonomía universitaria, en los términos del artículo 2.2.f de la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades (LOU). Esta misma norma en el párrafo tercero de su artículo 46 relativo a los derechos y deberes de los estudiantes, señala:



> 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.

Por otra parte, no es ocioso recordar que el artículo 13.2.c) del Real Decreto 1791/2010, de 30 de diciembre, por el que se aprueba el Estatuto del Estudiante Universitario, impone a los estudiantes el deber de «abstenerse de la utilización o cooperación en procedimientos fraudulentos en las pruebas de evaluación, en los trabajos que se realicen o en documentos oficiales de la universidad». Sin embargo, el artículo 5 de la misma norma ofrece una base insuficiente en esta materia ya que, al regular la evaluación se limita a señalar que esta «se ajustará a lo establecido en los planes docentes de las materias y asignaturas aprobados por los departamentos».

La cuestión, por tanto, consiste en dilucidar si el marco regulador, que se completa con normativas universitarias aprobadas por los Consejos de Gobierno, esto es disposiciones de carácter general y naturaleza reglamentaria, ofrecía un fundamento jurídico suficiente para el uso de sistemas de reconocimiento facial. Visto que las bases jurídicas aplicables no se basan en el consentimiento, resulta necesario considerar aspectos fuertemente interrelacionados. El tratamiento de cualquier dato personal debe superar el llamado principio protección de datos por defecto o juicio de minimización. Así el artículo 5.1.c) del RGPD ordena que los datos sean «adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados». Ello implica no solo un juicio que se proyecta sobre la naturaleza, volumen y

[15] Debe añadirse al equipo al profesor Julián Valero Torrijos, delegado de protección de datos de la Universidad de Murcia.

adecuación a la finalidad de los datos. Al suponer una limitación del derecho fundamental a la protección de datos exige una ponderación de los derechos, principios y/o valores constitucionales en conflicto tanto desde el punto de vista de la Constitución Española, como desde el punto de vista de la Carta de los Derechos Fundamentales de la Unión Europea.

La doctrina del Tribunal Constitucional al respecto de los límites a los derechos fundamentales posee un largo recorrido y arranca prácticamente con la tarea del propio Tribunal en la STC 11/1981. Muy sintéticamente expresada, esta doctrina exige la presencia de un fundamento constitucional de la medida, esto es, los límites deben estar expresamente formulados en el texto constitucional, y se interpretan restrictivamente. Además, la medida limitadora debe superar un doble juicio de congruencia y proporcionalidad ya que debe existir una mínima congruencia entre la medida restrictiva, el objetivo perseguido y el derecho limitado, y una proporcionalidad de la misma en términos de idoneidad e intervención mínima[16]. Este método, que también utiliza el Tribunal de Justicia de la Unión Europea, es tributario del modo en el que el Tribunal Europeo de Derechos Humanos ha afrontado la aplicación de los límites a los derechos fundamentales. En el caso del derecho a la vida privada del artículo 8 del Convenio Europeo de Derechos Humanos, este método interpretativo que se articula en tres etapas de análisis netamente diferenciadas. En primer lugar, se trata de determinar si realmente se ha producido una injerencia en el derecho al respeto de la vida privada y familiar, de su domicilio o de su correspondencia, para a continuación verificar si dicha intromisión se halla prevista por ley y si es legítima y necesaria de acuerdo con las excepciones del párrafo segundo del artículo 8 de la Convención.



Así pues, desde un punto de vista jurídico, los antecedentes normativos y la posición de la Agencia Española de Protección de Datos obligaban a considerar distintas posibilidades en relación con el uso de técnicas de reconocimiento facial en el desarrollo de un examen online. En nuestra opinión, un reconocimiento facial obligatorio que opera como condición necesaria para la realización de un examen no podría basarse en el consentimiento, salvo que se admitiese

[16] El fundamento jurídico sexto de la STC 57/1994, sintetiza esta doctrina:

> «no es ocioso recordar aquí que los derechos fundamentales reconocidos por la Constitución sólo pueden ceder ante los límites que la propia Constitución expresamente imponga, o ante los que de manera mediata o indirecta se infieran de la misma al resultar justificados por la necesidad de preservar otros derechos o bienes jurídicamente protegidos (SSTC 11/1981, fundamento jurídico 7., y 2/1982, fundamento jurídico 5., entre otras). Ni tampoco que, en todo caso, las limitaciones que se establezcan no pueden obstruir el derecho fundamental más allá de lo razonable (STC 53/1986, fundamento jurídico 3.). De donde se desprende que todo acto o resolución que limite derechos fundamentales ha de asegurar que las medidas limitadoras sean necesarias para conseguir el fin perseguido (SSTC 62/1982, fundamento jurídico 5., y 13/1985, fundamento jurídico 2.), ha de atender a la proporcionalidad entre el sacrificio del derecho y la situación en la que se halla aquél a quien se le impone (STC 37/1989, fundamento jurídico 7.) y, en todo caso, ha de respetar su contenido esencial (SSTC 11/1981, fundamento jurídico 10; 196/1987, fundamentos jurídicos 4. a 6.; 120/1990, fundamento jurídico 8, y 137/1990, fundamento jurídico 6.) ».

que el estudiante pudiera identificarse libremente utilizando otro método[17]. Y era poco probable, en el contexto de la pandemia, ofrecer una alternativa presencial que asegurase una elección libre por el estudiante[18].

Por ello debía considerarse, si el interés público esencial, definido en los términos del artículo 9.2.g) del RGPD[19], podría ofrecer una legitimación suficiente Para ello debería, no obstante, cumplir una serie de requisitos, a saber, la previsión por una norma con rango legal, -la LOU-, la proporcionalidad con el objetivo perseguido y la existencia de garantías adecuadas y específicas. Brevemente debemos señalar aquí que, sin una definición legal sobre el concepto de "interés público" o "interés general". En el ámbito del tratamiento de las llamadas categorías especiales de datos el Tribunal Constitucional se pronunció sobre esta materia en la conocida STC núm. 76/2019, que declaró inconstitucional el art. 58.bis).1 de la Ley Orgánica 5/1985, del Régimen Electoral General (LOREG). En esta sentencia la Corte Constitucional recordó no sólo la exigencia de un interés público recogido en una norma con rango de ley, que debería determinar la finalidad del tratamiento, sino que vino a señalar que dicha norma debería



[17] Cuestión que no obstante fue sometida en la referida consulta a la opinión de la Agencia Española de Protección de Datos.

[18] El llamado Working Party, también conocido como G29 o Grupo de Trabajo del artículo 29, -hoy Comité Europeo de Protección de Datos o EDPB por sus siglas en inglés-, señala en sus Directrices sobre el consentimiento que:

> «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. (…)
> 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.
> (…) Los desequilibrios de poder no se limitan a las autoridades públicas y a los empleadores, sino que también pueden producirse en otras situaciones. (…) El consentimiento no será libre en aquellos casos en los que exista un elemento de compulsión, presión o incapacidad para ejercer la libre voluntad.»

[19] Este dispone:

> **Artículo 9**
> **Tratamiento de categorías especiales de datos personales**
> 1. Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física.
> 2. El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes:
> (…)
> 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;

contener igualmente una serie de medidas adecuadas para garantizar el derecho a la protección de datos:

> las garantías adecuadas deben velar por que el tratamiento de datos se realice en condiciones que aseguren la transparencia, la supervisión y la tutela judicial efectiva, y deben procurar que los datos no se recojan de forma desproporcionada y no se utilicen para fines distintos de los que justificaron su obtención.

No obstante, el Tribunal Constitucional señala también, en este punto, que el nivel y la naturaleza de las garantías adecuadas «no se pueden determinar de una vez para todas» y que deben, por un lado, ser revisadas y actualizadas; y, por otro lado, que las mismas deben cumplir con el principio de proporcionalidad, buscando las posibilidades de tratamiento menos intrusivas, lo que variará, por lo tanto, en función del tipo de los datos y de su naturaleza (FFJJ 6º a 8º).



En la misma línea se pronunció la AEPD en su Informe jurídico 2018-0181 y en su Circular 1/2019, de 11 de marzo, destacando que las citadas garantías deberían señalar, entre otras cosas: el carácter excepcional de la medida; la necesidad de contar con una finalidad clara y determinada que legitime el tratamiento; la necesidad de determinar los sujetos que pueden realizar los tratamientos; y la necesidad de concretar los datos a ser tratados, así como los tratamientos y el momento en el que pueden producirse.

En principio, parece que podría invocarse como fundamento para el tratamiento la presencia de un interés público esencial habida cuenta de la trascendencia que poseía examinar online al conjunto de la población universitaria. Este interés no sería otro que el evaluar los conocimientos de los estudiantes a la vez que el de asegurar la identidad de la persona examinada y evitar el fraude, todos ellos previstos legalmente. Pero dicho interés debería reunir una serie de requisitos adicionales en términos de predeterminación normativa y garantías en los tratamientos. En este sentido, las referencias del artículo 46.3 de la LOU a la competencia de las universidades para establecer los procedimientos de verificación de los conocimientos de los estudiantes, o la referencia contenida en el Estatuto del Estudiante, no constituyen una previsión con una predeterminación normativa suficiente, clara y previsible, para la limitación de un derecho fundamental.

Precisamente por ello, el subgrupo de trabajo, integrado por delegados de protección de datos, consideró excluir de sus recomendaciones las técnicas de reconocimiento facial. Debido a su complejidad técnica, y al alto grado de exigencia que la legislación plantea el uso de datos biométricos, no era 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 obligaba a un proceso de interpretación de las habilitaciones para su uso que hizo 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.

### 3.3 El informe núm. 0036/2020 de la Agencia Española de Protección de Datos.

El informe de referencia, particularmente extenso, define el criterio del regulador en la materia, primero mediante una técnica autorreferencial[20] recuperando los posicionamientos que hemos expuesto en un epígrafe anterior. En segundo lugar, va definiendo una suerte de límites insoslayables en la aplicación del Reglamento General de Protección de Datos y la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales que en ocasiones subraya mediante texto en negritas[21]. El primero de ellos, es un posicionamiento reiterado en todas y cada de las notas de prensa emitidas desde marzo sobre tratamientos de datos personales y COVID-19.



> **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.**

Entrando en materia, la AEPD siguiendo con la metodología propia del análisis de riesgos, -aunque sin que conste a este autor que haya realizado ni una sola actividad de auditoría en los sistemas virtuales de las universidades españolas-, considera que existen riesgos en la implantación del reconocimiento facial en la evaluación online derivados «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». Afirmaciones todas, que pueden compartirse o no, pero que en nuestra opinión constituyen meras preconcepciones. En cualquier caso, la AEPD "*a limine"* realiza una advertencia, que cualquier delegado de protección de datos medianamente avezado sabe que debe interpretar poco menos que como derecho positivo:

> esta Agencia considera necesario realizar una advertencia con carácter general[22], 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**

[20] En este sentido el regulador suele utilizar sus informes previos prácticamente del mismo modo en el que los tribunales invocan su jurisprudencia.

[21] Esta técnica resulta cuando menos curiosa y es reiteradamente utilizada en el documento. Tal vez, el regulador la considere una manera pedagógica de asegurar que la sociedad y los operadores jurídicos identifiquen los mensajes esenciales.

[22] El subrayado es nuestro, nótese el contundente tono que emplea la Agencia Española de Protección de Datos.

> **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**.



Sin perjuicio del estilo, es evidente la manifiesta oposición de la Agencia Española de Protección de Datos al uso de técnicas de reconocimiento facial. Asimismo, el Informe indica sin ningún género de dudas 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».

Desde el punto de vista de las condiciones jurídicas que legitimarían el tratamiento de tales datos la Agencia Española de Protección de Datos excluye el consentimiento en la medida en la que «el alumno no se encuentra en situación de igualdad con la universidad en la que estudia»[23]. Más relevante resulta sin duda su interpretación restrictiva de la aplicación del principio de interés público como causa de legitimación. Para ello, se define como requisito que «las normas internas de la Universidad prevean la grabación de los exámenes orales»[24], en cuyo caso el tratamiento se encontrará fundamentado en lo previsto en el artículo 6.1.e) del

---

[23] En este sentido señala:

> «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.**»

[24] Sorprende esta aseveración en la medida en la que la propia Agencia Española de Protección de Datos, más adelante es más restrictiva con cita expresa de la doctrina del fundamento jurídico undécimo de la STC núm. 292/2000 del Tribunal Constitucional sobre reserva de ley.

RGPD siendo necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Pero, añade que:

> **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.**



La Agencia Española de Protección de Datos, se apoya en la STC 76/2019 a fin de subrayar el doble requisito para la concurrencia del interés público esencial al que se refiere el artículo 9.2.g) del RGPD. Esto es la predeterminación normativa en una norma con rango de Ley que debe incluir las garantías adecuadas de tipo técnico, organizativo y procedimental, que prevengan los riesgos derivados del tratamiento[25]. Esto implica que la ley reguladora reúna ciertas características:

> **« 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.**

[25] En efecto el fundamento jurídico octavo de la sentencia señala:

> «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»

**Además, dicha ley deberá respetar en todo caso el principio de proporcionalidad (…)»**

Como conclusión, la Agencia Española de Protección de Datos considera el artículo 46.3 de la LOU «insuficiente para permitir la utilización de técnicas de reconocimiento facial en los procesos de evaluación, al no cumplir los requisitos anteriormente señalados».

### 3.-El necesario desarrollo legislativo: ¿una conclusión imposible?

La consecuencia ulterior del posicionamiento del regulador no es otra que la necesidad de reformar la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades para acoger este tipo de tratamientos. En este sentido resulta significativa la previsión en el modelo francés del "Décret no 2017-619 du 24 avril 2017 relatif à la mise à disposition d'enseignements à distance dans les établissements d'enseignement supérieur". Esta norma modificó el Código de la Educación regulando la educación a distancia[26] y sentó las bases para la aplicación de controles en los exámenes online:



> Art. D. 611-12. – Les conditions de la validation des enseignements, dispensés en présence des usagers ou à distance, le cas échéant sous forme numérique, sont arrêtées dans chaque établissement d'enseignement supérieur au plus tard à la fin du premier mois de l'année d'enseignement et elles ne peuvent être modifiées en cours d'année.
>
> La validation des enseignements contrôlée par des épreuves organisées à distance sous forme numérique, doit être garantie par:
>
> 1º La vérification que le candidat dispose des moyens techniques lui permettant le passage effectif des épreuves;
>
> 2º La vérification de l'identité du candidat;
>
> 3º La surveillance de l'épreuve et le respect des règles applicables aux examens.»

La experiencia francesa ofrece un modelo para una posible reforma legislativa nacional. No obstante, esta debería incluir al menos las siguientes cautelas adicionales en términos de medidas y garantías:

- La obligatoriedad del desarrollo de una evaluación de impacto relativa a la protección de datos sobre el uso de este tipo sistema de información.
- Asegurar una adecuada disponibilidad de medios por parte de los estudiantes concernidos.
- Disponer de procedimientos que permitan resolver errores de identificación y fallos en los sistemas.

[26] Así:

> «*Art. D. 611-11.* – Constitue un enseignement de l'enseignement supérieur à distance un enseignement délivré en dehors de la présence physique dans un même lieu que l'étudiant de l'enseignant qui le dispense. Cet enseignement est totalement ou majoritairement conçu et organisé par des enseignants de l'établissement qui le propose. «Un enseignement à distance est assorti d'un accompagnement personnalisé des étudiants».

▪ Asegurar la aplicación de los estándares de seguridad más exigentes de los previstos en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

▪ Incentivar la responsabilidad proactiva de la institución universitaria en al menos dos ámbitos estratégicos:

- La formación del personal.

- La contratación diligente de terceros, encargados del tratamiento.

Sin embargo, la Agencia Española de Protección de Datos en el Informe analizado en el epígrafe anterior, se refiere de modo expreso a una posible futura legislación. A tal respecto señala:



> 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.

El mensaje del regulador resulta claramente entendible: siempre que el profesor pueda reconocer visualmente a cada estudiante no se aplicarán tecnologías de reconocimiento facial. En caso de extraordinaria urgencia y necesidad, -como en una pandemia que nos confine a todos-, y sólo para algunas asignaturas se admitiría eventualmente el uso de estas técnicas. Resulta sin duda una posición singular. En este sentido, el derecho fundamental a la protección de datos prevalece de modo absoluto sobre las garantías ordenadas a evitar el fraude académico. Estas, en plena transformación digital deberán articularse a través de medios del Siglo XX. La universidad, así se declara en el informe, no es una institución confiable, ni segura, e incluso en aquellos casos en los que su oferta sea completamente virtual debe invertir en disponer de recursos presenciales si desea examinar a sus estudiantes con ciertas garantías.

Nadie alberga ya dudas sobre la posición e influencia de la AEPD. Parece, sin embargo, que erigirse en protolegislador, cuestionar la confiabilidad de la universidad y determinar inexorablemente sus decisiones organizativas no sea una buena noticia para la autonomía de las universidades y anuncie una ingente labor al ministerio del ramo.

**BIBLIOGRAFÍA**

▪ AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS-AEPD y EUROPEAN DATA PROTECTION SUPERVISOR-EDPS (2020). *14 equívocos con relación a la identificación y autenticación biométrica*. Disponible (30/09/2020) en https://www.aepd.es/es/guias-y-herramientas/guias

▪ COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS-CNIL (2109). *Reconnaissance faciale: pour un débat à la hauteur des enjeux*. Disponible (30/09/2020) en https://www.cnil.fr/fr/reconnaissance-faciale-pour-un-debat-la-hauteur-des-enjeux

▪ DE HERT, P y SPROKKEREEF, A (2007). Ethical practice in the use of biometric identifiers within the EU. *Law, Science and Policy, Vol. 3,* pp. 177–201.

▪ EUROPEAN DATA PROTECTION BOARD. Guidelines 05/2020 on consent under Regulation 2016/679. Version 1.1. Adopted on 4 May 2020. Disponible (30/09/2020) en https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf.

▪ GONZÁLEZ, M. MARCO, E. y MEDINA, T. (2020). *Informe de iniciativas y herramientas de evaluación online universitaria en el contexto del Covid-19*. Gabinete del Ministro de Universidades. Disponible (30/09/2020) en https://www.usal.es/files/Informe_modelos_evaluacion_Gabinete_ministro_universidades.pdf

▪ GRUPO DE RESPONSABLES DE DOCENCIA ONLINE DE LAS UNIVERSIDADES PÚBLICAS DE CASTILLA Y LEÓN. (2020). *Guía de recomendaciones para la evaluación online en las Universidades Públicas de Castilla y León*. Disponible (30/09/2020) en https://virtuva.uva.es/recursos/docs/GuiaRecomendacionesEvaluacionOnline.pdf

▪ GRUPO DE TRABAJO DEL ARTÍCULO 29. Dictamen 3/2012 sobre la evolución de las tecnologías biométricas (00720/12/ES WP193). Disponible (30/09/2020) en https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_es.pdf.

▪ GRUPO DE TRABAJO INTERSECTORIAL DE CRUE UNIVERSIDADES. *Informe del Grupo de Trabajo Intersectorial de Crue Universidades sobre Procedimientos de Evaluación no Presencial. Estudio del Impacto de su Implantación en las Universidades Españolas y Recomendaciones Españolas*, Versión 1.0 de jueves 16 de abril de 2020. Disponible (30/09/2020) https://www.crue.org/informes-y-posicionamientos/

▪ Informes Jurídicos de la Agencia Española de Protección de Datos núms. 0392/2011, 0186/2017, 0181/2018, 0063/2019 y 0036/2020. Disponibles (30/09/2020) en https://www.aepd.es/es/informes-y-resoluciones/informes-juridicos.



▪ MARTÍNEZ MARTÍNEZ, R., ARENAS RAMIRO, M, y PASCUAL GUMBAU, J. (2020) Informe sobre el impacto normativo de los procedimientos de evaluación online: protección de datos y garantía de los derechos de las y los estudiantes. Madrid, CRUE, pág. 26. Disponible (30/09/2020) en https://www.usal.es/files/wp_cumplimiento.eval_.pdp_-_rm-ma-jpg.final-2020.04.15.pdf.pdf

▪ MARTÍNEZ MARTÍNEZ, R (2020). Autoridades independientes, no irresponsables, en el País-Cinco Días. Disponible (30/09/2020) en https://cincodias.elpais.com/cincodias/2020/05/25/legal/1590385284_647173.html.

▪ SUREDA NEGRE, y COMAS FORGAS, R. (2020). La promoción del fraude académico a través de los buscadores. *The Conversation*. Disponible (29/09/2020) en https://theconversation.com/la-promocion-del-fraude-academico-a-traves-de-los-buscadores-141593.