I.S.S.N.: 1138-2783

Sobre el uso de tecnologías de reconocimiento facial en la universidad: el caso de la UNED

(On the Use of Facial Recognition Technologies in University: the UNED Case)

José L. Aznarte
Mariano Melendo Pardos
Juan M. Lacruz López
Universidad Nacional de Educación a Distancia, UNED (España)

DOI: https://doi.org/10.5944/ried.25.1.31533

Cómo referenciar este artículo:
Aznarte, J. L., Melendo Pardos, M., y Lacruz López, J. M. (2022). Sobre el uso de tecnologías de reconocimiento facial en la universidad: el caso de la UNED. *RIED. Revista Iberoamericana de Educación a Distancia, 25*(1), pp. 261-277. https://doi.org/10.5944/ried.25.1.31533

Resumen

Las tecnologías de identificación biométrica han experimentado un gran desarrollo en los últimos años, siendo aplicadas a decenas de ámbitos diferentes, entre los que se encuentra el ámbito educativo, en particular el universitario. Sin embargo, en este artículo argumentamos que dicha tendencia puede impactar de formas inesperadas a los procesos de enseñanza/aprendizaje. Así, se exponen algunas consideraciones principales acerca del uso de tecnologías de identificación biométrica en general y más particularmente de técnicas de reconocimiento facial en el marco de los exámenes universitarios, prestando especial atención al problema de realizar los exámenes presenciales por medios remotos durante la pandemia de la COVID-19. Se ofrece un análisis general de las limitaciones de esta tecnología en sus dimensiones técnica, jurídica y ética, y se exploran las posibles consecuencias, en esas tres dimensiones, del uso de dichas tecnologías. A modo de ilustración, se toma el caso concreto de la UNED, la universidad más grande del Estado español, exponiendo las decisiones tomadas por esta institución para dar respuesta al desafío que supusieron las restricciones de movimiento durante el estado de alarma. Dado el gran número de evidencias de que esta tecnología está aquejada de graves problemas con impredecibles consecuencias, en todo caso se recomienda observar el principio de precaución y tomar decisiones con la máxima cautela.

Palabras clave: evaluación; tecnologías de la información; ética; prevención; fraude.

Abstract

Biometric identification technologies have experienced a boom in recent years, with applications being proposed and implemented in a wide array of fields, including education and, in particular, at the university level. However, in light of recent experiences, it is a fact that such trend might impact learning and teaching processes in unexpected ways. In that sense, we summarize some considerations about the use of biometric identification technologies in general and, particularly, about the use of facial recognition technologies in the framework of remote assessment during the COVID-19 pandemic. We provide a general analysis of the limitations of those technologies, with special attention to the technical, legal and ethical dimensions, and we explore potentially negative consequences of the use of such technologies. As an illustration, the experience of UNED, the biggest university in Spain, with a hybrid face-to-face and remote learning and teaching system, is provided. We expose the decisions taken by this institution to face the challenge of remote examination during the imposed lockdowns due to COVID-19. Given the number of evidences pointing to acute flaws in the technology which might have unpredictable consequences, in any case it is recommended to apply extreme caution in making decisions in this field.

Keywords: evaluation; information technologies; ethics; prevention; fraud.

En los últimos años, las tecnologías de reconocimiento facial –en adelante TRF– y, en general, las tecnologías de identificación biométrica, están expandiéndose a gran ritmo (Montag et al., 2021). Sin embargo, hay evidencias crecientes de que estas tecnologías pueden causar serios perjuicios, especialmente a personas desfavorecidas socialmente y racializadas.

De hecho, la Unión Europea, en el marco del desarrollo del Libro Blanco sobre Inteligencia Artificial, está actualmente estudiando la imposición de una moratoria a todos los usos de las TRF en dominios de alta sensibilidad política o social, incluyendo no solo vigilancia y policía, sino también en la educación y el empleo[1]. El hecho es que, en estos campos, las TRF suponen riesgos y consecuencias que no podrían ser remediadas de forma retroactiva (Crawford et al., 2019; Izquierdo, 2020). Dicha moratoria se plantea con el fin de permitir a investigadores y legisladores la realización de una valoración sosegada de la mejor aproximación posible a la restricción y la regulación de las TRF, así como para dar tiempo a las comunidades sobre las que tales tecnologías serán aplicadas a fin de que hagan sus propias evaluaciones acerca de su implantación.

Por otro lado, en lo que es una muestra de la gravedad del asunto, un buen número de ciudades y estados de EE.UU.[2], entre ellas San Francisco, Berkeley y Oakland, han legislado y activado ya sus propias prohibiciones para evitar que instituciones gubernamentales hagan uso de las TRF.

En este marco, la irrupción de la pandemia de COVID-19 y la necesidad de limitar todo tipo de actividades presenciales, trasladándolas al ámbito virtual, trajeron

RIED. Revista Iberoamericana de Educación a Distancia (2022), 25(1), pp. 261-277.
DOI: https://doi.org/10.5944/ried.25.1.31533 – ISSN: 1138-2783 – E-ISSN: 1390-3306

consigo un interesante debate sobre los cambios necesarios al proceso de evaluación (García-Peñalvo et al., 2020) y en concreto sobre la posibilidad de que la universidad utilizara las TRF como garantía en la realización de sus pruebas online durante los cursos 2019/2020 y 2020/2021. Se planteó por ello con urgencia la necesidad de evaluar este contexto de incertidumbre y de críticas fundadas hacia las tecnologías de identificación biométrica en general y, más en concreto, hacia las TRF, con el objeto de determinar el método de evaluación más adecuado para los estudiantes universitarios. En este documento, se expone el caso concreto de la UNED, que es la mayor universidad española y una de las más grandes de Europa, y que se caracteriza justamente por su modelo semipresencial (Aznarte y Lacruz, 2021).

En la elaboración de esta investigación se ha seguido una metodología de revisión sistemática del estado de la cuestión, atendiendo a tres dimensiones principales. Por un lado, se ha revisado toda la información disponible acerca de herramientas software existentes, bajo la perspectiva técnica de la ingeniería del software y del desarrollo de la inteligencia artificial. Esta perspectiva ha sido complementada con una mirada técnica desde el derecho, en la que se ha revisado tanto la normativa vigente como la jurisprudencia existente. Finalmente, una tercera dimensión ha tenido en cuenta la perspectiva de la prevención y la resolución de conflictos que realizan cotidianamente los órganos universitarios encargados de dicha tarea (inspección de servicios, habitualmente).

EL RECONOCIMIENTO FACIAL EN EDUCACIÓN

La idea de delegar en la tecnología los medios para garantizar la limpieza en los exámenes, una vez que estos han debido ser trasladados al ámbito virtual, entronca con un sentido común bastante extendido en nuestros días. Existen aplicaciones de uso cotidiano basadas en la identificación biométrica (el desbloqueo de ciertos terminales de teléfono móvil, por ejemplo), a la vez que existen multitud de otras aplicaciones comerciales que aspiran a convertirse en habituales (*check-in* automático en los aeropuertos, por ejemplo). Como veremos, en el ámbito de la educación, algunos países usan estas tecnologías para el préstamo en bibliotecas, sistemas de pago, apertura de taquillas y otros usos.

Más allá, según sus promotores, el uso de tecnologías biométricas podría conllevar un número de ventajas adicionales en el marco de la educación. Gracias a ellas se promovería un uso más eficiente del tiempo, ahorrando trámites como el control de asistencia y facilitando la adaptación curricular para estudiantes ausentes. Se podría incrementar la seguridad en las aulas, detectando de forma automática a personas ajenas al curso (bajo la premisa de que dichas personas podrían entrañar riesgos para quienes sí están matriculados) (Montgomery y Marais, 2014). También, combinando la biometría con la inteligencia artificial, se podría inferir la implicación de cada estudiante, así como posibles problemas de comportamiento (Dewan et al., 2019). Pero quizá la mayor reivindicación de estas tecnologías sea la relacionada

con la garantía de la integridad académica: poder asegurar que alguien es quien dice ser, en un proceso de enseñanza/aprendizaje, es la aspiración central de quienes desarrollan y venden estas tecnologías (Valera et al., 2015; Hernández et al., 2008; Apampa et al., 2010).

Así, las aplicaciones de la biometría y la inteligencia artificial en la educación han visto un enorme desarrollo en los últimos años. Este es el caso de las TRF (Valera et al., 2015), que están siendo sometidas a un gran desarrollo comercial a la vez que están siendo cuestionadas por parte de la comunidad científica (Andrejevic y Selwin, 2019).

Algunas de estas críticas giran en torno a la aplicación de las TRF en la seguridad de los campus. Esta forma de TRF es más común en los EE.UU., donde los ataques con armas en las escuelas han provocado que las autoridades educativas gasten 27.000 millones de dólares en sistemas de seguridad para los campus (Doffman, 2018).

Sin embargo, cada vez más voces alertan contra la naturaleza deshumanizadora de estas aplicaciones, cuyos fundamentos estadísticos tienden a ser inherentemente reduccionistas de la complejidad y la diversidad. También hay grandes prevenciones respecto al hecho de que el género y la raza del alumnado es traído a un primer plano por las TRF, dado que la forma en que estas tecnologías esquematizan el rostro humano implica "cálculos" de género y raza como medios para dividir arbitrariamente a la población, lo que puede ser considerado como una práctica discriminatoria. Según Stark (2019), «si la sociedad no fuera racista, las TRF nos inclinarían hacia el racismo; dado que la sociedad es racista, las TRF exacerban esa actitud».

De la misma manera, otras voces alertan sobre la contribución de las TRF a la naturaleza cada vez más autoritaria de la educación, sobre la erradicación de espacios "oscuros" en los que ciertos tipos de alumnado deben poder refugiarse, sobre la lógica en cascada de la automatización que se basa en la recopilación creciente de datos "por si acaso" o la arriesgada estandarización que puede conllevar dinámicas de opresión contra grupos concretos, entre otras muchas críticas (Valera et al., 2015)[3,4].

EL RECONOCIMIENTO FACIAL EN LA UNED

La evaluación en la UNED

Dejando a un lado los procesos de evaluación continua (que afortunadamente cada vez tienen más peso), la evaluación en la UNED siempre ha estado mediada por la presencialidad: todos los exámenes finales se realizan normalmente en la extensa red de Centros Asociados. En cada convocatoria, se forman tribunales compuestos por miembros del PDI (Personal Docente e Investigador) cuya labor es organizar las pruebas y garantizar la limpieza del proceso. Cada examen de cada asignatura se realiza de forma síncrona en todos los Centros Asociados, y el alumnado puede elegir dónde realizar sus pruebas. En este esquema, la presencialidad es entendida como

RIED. Revista Iberoamericana de Educación a Distancia (2022), 25(1), pp. 261-277.
DOI: https://doi.org/10.5944/ried.25.1.31533 – ISSN: 1138-2783 – E-ISSN: 1390-3306

garantía de calidad, y es comúnmente considerada como un activo importantísimo para la institución.

Con la llegada de las restricciones de movimiento derivadas de la pandemia, obviamente este esquema entró en crisis: no siendo posible organizar los exámenes de la forma habitual, fue necesario desarrollar, con muy poco tiempo, una alternativa que permitiera trasladar los exámenes a la red. El mantenimiento de la calidad y la introducción de las mínimas modificaciones posibles respecto al proceso habitual fueron los criterios de diseño de dicha solución. En ese marco, las TRF fueron propuestas como herramienta principal.

El reconocimiento facial y el marco ético de uso de datos masivos

Con anterioridad al planteamiento de la situación que ahora analizamos, la UNED realizó una consulta a toda la comunidad universitaria[5] en la que sometió a su deliberación un conjunto de cautelas básicas para el uso de datos masivos en la propia universidad y que afecta directamente a la discusión sobre el empleo de las TRF en nuestra actividad académica (Aznarte, 2020). Estas cautelas y el marco teórico que las soporta están descritas en el documento "Consideraciones éticas en torno al uso de tecnologías basadas en datos masivos"[6].

Durante este proceso participativo, casi 2.500 miembros de la comunidad universitaria mostraron su apoyo a las cautelas propuestas –con un total de casi 7.500 apoyos– o deliberaron sobre ellas en casi 300 hilos de debate. También se propusieron 25 nuevas cautelas suplementarias a las 9 que se ofrecían al inicio. Todos estos aportes están siendo estudiados con detalle para integrar aquellos que gocen de más consenso en un documento final que pueda ser asumido por la institución. Lo que es indiscutible es que la comunidad universitaria se siente interpelada por la implantación de tecnologías basadas en datos masivos y está vigilante en este ámbito.

Es obvio que las tecnologías de identificación biométrica entran de lleno en el ámbito de las tecnologías basadas en datos masivos, y por tanto están afectadas por todos los riesgos de estas. Por ello, en el ámbito de la discusión sobre las características del modelo de evaluación online sería difícil de justificar hacia el alumnado que en la aplicación de cualquier sistema basado en TRF no se observaran todas las cautelas establecidas en el marco ético, y es probable que de no actuar con respeto a las mismas se produjera una crisis de reputación de gran alcance público.

Un análisis de dicho marco ético revela que el empleo de las TRF en un sistema de evaluación online puede producir conflictos al menos con las siguientes cautelas:

3. Del consentimiento / «El consentimiento de cada miembro de la comunidad universitaria será necesario para el uso de sus datos personales»: Esta cautela tiene implicaciones en el proceso de recolección de los datos faciales y de la autorización del estudiantado para su empleo en las pruebas online. En primer lugar, por la situación de dependencia del estudiantado frente a las decisiones de

la autoridad académica. Pero, además, porque este tipo de situaciones provoca un desequilibrio claro entre los dueños de los datos y quienes controlan esa información una vez cedida. Ambos aspectos, como veremos posteriormente, han sido señalados por la Agencia Sueca de Protección de Datos.

6. De la validez y la fiabilidad / «Para asegurar que las aplicaciones de tecnologías basadas en datos son válidas y fiables, la UNED garantizará que los datos son precisos y representativos de aquello que dicen medir»: Con respecto a esta cautela, tal y como veremos en el siguiente apartado, las imprecisiones y limitaciones de las TRF comprometen gravemente su cumplimiento, incidiendo tanto en la fiabilidad de los resultados como en el debido respeto al principio de igualdad.
7. De los posibles impactos adversos / «La UNED reconoce que cualquier individuo es siempre más que la suma de los datos disponibles acerca de ella o él, y que las circunstancias personales no pueden ser descritas totalmente por los datos»: Las fricciones de las TRF en este ámbito resultan especialmente significativas teniendo en cuenta las prevenciones que su uso plantea entre la comunidad científica.
8. De la participación / «Siempre que sea posible, la UNED tratará de involucrar a los distintos colectivos de la comunidad universitaria en la aplicación de tecnologías basadas en datos»: Se llevó a cabo una encuesta a los alumnos sobre el tema, sin embargo, este esfuerzo no supone el cumplimiento de la octava cautela puesto que, además de la reducida muestra –tan solo contestaron el 10% de los estudiantes–, esta está evidentemente sesgada hacia las personas más proclives a la utilización de las TIC. Un proceso participativo es algo más serio y requiere su tiempo. Pese a la aprobación del estado de alarma no debemos prescindir de modo radical de los procedimientos. Los procedimientos no son solo cuestiones formales, sino que reflejan elementos profundos de nuestra visión de nosotros mismos y nuestras relaciones –ejemplo: ¿qué diferencias sobre la comprensión de cada sujeto y su posición respecto a los demás implican una elección democrática, un sorteo al estilo de la antigua Grecia para algunos cargos, o una designación a dedo? En el fondo da lo mismo lo que implican, pero sirve para poner de manifiesto que conciben los sujetos sociales y sus relaciones de forma muy diferente–.

Riesgos del uso de tecnologías de reconocimiento facial en la universidad

Pero no solo desde la ética, las TRF plantean serios problemas en su aplicación. A continuación, se ofrece una lista no exhaustiva de los potenciales asuntos que deben preocupar a cualquier institución educativa a la hora de valorar la adopción de sistemas de identificación biométrica[7]:

RIED. Revista Iberoamericana de Educación a Distancia (2022), 25(1), pp. 261-277.
DOI: https://doi.org/10.5944/ried.25.1.31533 – ISSN: 1138-2783 – E-ISSN: 1390-3306

A. No existe un marco regulatorio claro para las TRF

La mayor parte de los países carecen de legislación específica que regule el uso de las TRF, y ese es el caso del Estado español. En la Ley Orgánica de Protección de Datos[8] (LOPD) y en el Reglamento Europeo de Protección de Datos[9] (RGPD) no hay un apartado específico sobre el reconocimiento facial, si bien se habla de datos biométricos identificativos –como el rostro–. Aunque es cierto que el Grupo del artículo 29 del RGPD sí tiene algunas recomendaciones y lo mismo ocurre con el Dictamen 3/2012 sobre la evolución de las tecnologías biométricas, también es cierto que dichas recomendaciones no han sido trasladadas a la legislación y que, además, no existe jurisprudencia al respecto (Martínez, 2020).

No obstante, el año 2019, la DPA, Agencia de Protección de Datos de Suecia, sancionó a un colegio sueco con una multa de unos 18.500 euros, por utilizar la tecnología facial para el reconocimiento de sus alumnos, a pesar de contar con el consentimiento expreso de estos. En su resolución, la DPA considera que la actuación del colegio supone la violación de varios artículos del RGPD, señalando que el consentimiento no es una vía legal para justificar el empleo de tal tecnología por dos razones: el desequilibrio claro entre los dueños de los datos y quien controla esta información tras su recolección; y la situación de dependencia con respecto a la dirección del centro en que se encuentran los estudiantes.

En todo caso, el RGPD establece que, para el tratamiento de este tipo de datos, es necesario realizar previamente una evaluación de impacto, y que el responsable del tratamiento debería implementar sistemas de anonimización o seudonimización y cifrado de los datos, así como la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.

En el caso objeto de análisis, en el supuesto de que se hubieran podido cumplimentar los requisitos técnicos en un periodo de tiempo tan breve como el que existía entre el planteamiento del problema y la celebración de las pruebas, resultaba altamente improbable que se hubiera podido realizar una evaluación de impacto con garantías. En definitiva, difícilmente podrían ser cumplimentados los requerimientos del RGPD antes de lanzar el sistema.

B. El empleo de las TRF puede suponer una violación de los principios de necesidad y proporcionalidad

Un principio comúnmente aceptado y reconocido por la ONU entre los derechos humanos más básicos es que la vigilancia debe ser necesaria y proporcionada[10]. En la misma línea, desde que en los años 90 del pasado siglo nuestro Tribunal Constitucional adoptó el denominado “test alemán” en el examen del principio de proporcionalidad (Lascuraín, 2020), es una constante en su jurisprudencia que

las medidas que afecten a derechos fundamentales deben ser idóneas o adecuadas, necesarias y proporcionadas en sentido estricto[11] (Perelló, 1997; Roca, 2013).

Podemos partir de la base de que la utilización de las TRF para la realización de las pruebas de evaluación superaría el test de idoneidad, en cuanto que se perseguiría un fin legítimo con un medio que podría alcanzar el resultado pretendido. Pese a que incluso en este primer componente del principio de proporcionalidad podrían señalarse algunos problemas (Ferguson, 2021), la utilización de las TRF podría aparecer, desde esta perspectiva instrumental, como un medio adecuado para un fin legítimo. Sin embargo, muchos más problemas plantean los subprincipios de necesidad y proporcionalidad en sentido estricto.

Con respecto a la necesidad del empleo de las TRF en las pruebas de evaluación que coincidieron con las restricciones de movimiento impuestas por la pandemia, esto es, la inexistencia de medios menos lesivos o incisivos para los derechos fundamentales, nos enfrentábamos a dos opciones: implementar un nuevo sistema de evaluación para salir de una situación excepcional –que puede mejorar con el tiempo, lo que implica que puede ser innecesario actuar ahora para evitar el posible mal futuro– o mantener el sistema de exámenes habitual, de calidad acreditada. Esto es, nos enfrentábamos al dilema de optar por el mantenimiento de la estructura temporal, con los interrogantes que hemos visto que implica, frente al de asegurar la metodología y calidad contrastada del proceso de evaluación presencial.

Ahora bien, para justificar la necesidad de la prueba es preciso determinar que no hay medidas menos gravosas que puedan garantizar el mismo resultado o uno equivalente. En este aspecto, la posibilidad de posponer la celebración de los exámenes o de desarrollar un sistema de evaluación online que no incluyera las TRF cuando menos debilitaba la idea de que el empleo de las mismas en una evaluación online sea necesario. La posibilidad de utilizar un diseño diferente de las pruebas y mecanismos de evaluación, orientados a minimizar la posibilidad de éxito del uso de medios fraudulentos, posibilidad realmente existente, pone seriamente en cuestión, si no niega directamente, la necesidad de acudir a las TRF[12].

Y en cuanto a la cuestión de la proporcionalidad en sentido estricto (Navarro, 2010), esto es, que la medida no produzca más perjuicios de los beneficios que ofrece –incluido el efecto desaliento–, si tenemos en cuenta que cualquier preferencia por unos intereses solo legitima el menor perjuicio posible de otros intereses afectados –en este caso, las supuestas garantías de la aplicación de las TRF, frente a la privacidad de los estudiantes y la calidad del sistema de evaluación–, concluiremos que no nos encontramos con una medida proporcionada, ya que existen medidas menos gravosas con las que llegar a una solución adecuada del problema (véase también AEPD, 2020).

DOI: https://doi.org/10.5944/ried.25.1.31533 – ISSN: 1138-2783 – E-ISSN: 1390-3306

C. Las TRF pueden violar el derecho a la privacidad del alumnado

Incluso en los espacios públicos debe preservarse el derecho a la privacidad. Pese a que la vigilancia durante un examen es algo no solo lícito, sino necesario para garantizar la corrección del proceso de evaluación, el hecho de que la universidad se dote de la capacidad de reconocer al alumnado por su rostro podría suponer un menoscabo de ese derecho, ya que implica que los estudiantes puedan ser vigilados en otros momentos.

A diferencia de otros tipos de datos personales, los datos faciales se prestan a una vigilancia constante y permanente. En pocas palabras: las personas están permanentemente conectadas con sus caras. A diferencia de la participación en redes sociales o de las interacciones mediante los cursos virtuales, no existe una opción para que el alumnado restrinja qué datos "comparten". A ello se suma la gran cantidad de datos de los concretos estudiantes con los que cuenta la universidad –edad, género, domicilio, etc...–, que junto con las TRF acabarían por conformar una descripción detallada de cada uno de ellos.

Además, en el concreto caso que nos ocupa, habría sido necesario resolver la captura inicial de datos biométricos y su validación: si bien es de suponer que la práctica totalidad del alumnado ha adjuntado su foto a la matrícula, dicha foto no tiene por qué estar digitalizada en todos los casos y, lo que es más grave, no tiene por qué estar en posesión de la Sede Central. Esto es, el proceso de implementación de un sistema de TRF para la realización de exámenes online no solo plantea obstáculos y dudas teóricas y jurídicas, sino que resulta claramente más complejo que la mera creación de un software.

D. Las TRF son imprecisas y el software falible

La promesa de la inteligencia artificial aplicada al reconocimiento facial es que se pueden obtener resultados de gran precisión. Sin embargo, muchos estudios[13,14] han puesto de relieve cómo los algoritmos entrenados sobre datos sesgados en cuanto a raza tienen dificultades para identificar a personas racializadas, especialmente mujeres. Este sesgo algorítmico es particularmente preocupante si resulta en discriminaciones contra personas pertenecientes a minorías vulnerables (Ferguson, 2021).

Más allá de la imprecisión, nos topamos con la falibilidad del software. ¿Qué ocurre si durante el examen falla el programa, o el reconocimiento facial, o la conexión, o el equipo se bloquea porque es muy antiguo? ¿Se pasa por alto la incidencia? ¿Se anula el examen para esa persona? ¿Se asume que ha provocado intencionadamente un problema para poder copiar al menos durante un rato? Conociendo el comportamiento habitual del software comercial, es temerario no considerar la inmensa casuística de la informática en un momento como ese.

En los últimos tiempos hemos tenido algunos ejemplos claros de fallos en los sistemas informáticos de instituciones educativas. El rigor en el proceso de evaluación de las tecnologías ofertadas no puede ser sustituido por la palabra de quien está comercialmente interesado en la venta de una aplicación.

E. Las TRF pueden dar lugar a sesgos de automatización

Está demostrado que quienes hacen uso de TRF tienden a asumir ciegamente que dichas tecnologías son infalibles, y esto puede dar lugar a decisiones muy equivocadas[15]. Este sesgo de automatización debe ser evitado: las decisiones basadas exclusivamente en criterios automatizados no deben determinar cómo las instituciones educativas tratan al alumnado. La intervención humana debe ejercer un control significativo y revisar las decisiones automáticas antes de considerarlas válidas.

F. Las TRF pueden producir discriminaciones y vulneraciones del principio de igualdad

Con respecto al respeto al principio de igualdad, el primer escollo está en el modo en que se instalaría cualquier aplicación de TRF y la(s) foto(s) en que se basa. Si se requiere que el alumnado establezca unos ciertos permisos o configuraciones, estaríamos ante la primera oportunidad de discriminación, ya que no todos se sentirían capaces de poner su equipo informático a punto, particularmente quienes no poseen formación informática y sobre todo las personas de edad avanzada.

Otra fuente de discriminación es la calidad de la conexión y del equipo. Efectivamente esto afectaría particularmente a personas de bajos ingresos, pero también a otras (Rodicio-García et al., 2020).

En el caso particular de la UNED, todo ello afecta sensiblemente a una de sus características nucleares. El art. 4 a) de los estatutos señala, como función específica de la universidad, la de:

> *«Facilitar el acceso a la enseñanza universitaria y la continuidad de sus estudios a todas las personas capacitadas para seguir estudios superiores que elijan el sistema educativo de la UNED por su metodología o bien por razones laborales, económicas, de residencia o cualquier otra.»*

A ello se suma el art 143 h), que recoge el derecho de los y las estudiantes:

> *«A la igualdad de oportunidades y no discriminación por razones de sexo, raza, religión o discapacidad o cualquier otra condición o circunstancia personal o social en el acceso a la Universidad, ingreso en los centros, permanencia en la universidad y ejercicio de sus derechos académicos.»*

DOI: https://doi.org/10.5944/ried.25.1.31533 – ISSN: 1138-2783 – E-ISSN: 1390-3306

Así, no parece justo cambiar la forma de examinar y, sobre todo, hacerlo por un sistema que puede perjudicar a los más desfavorecidos económicamente.

Por otro lado, no es conveniente descartar que la sobrecarga de la recogida de datos biométricos, la puesta a punto de los sistemas, los posibles ensayos previos etc., desanimaría a muchos potenciales participantes y, en particular, a quienes estuvieran teniendo durante la crisis provocada por la pandemia particulares dificultades al teletrabajar y soportar cargas de cuidados o por sufrir ansiedad, desánimo o depresión –de nuevo, el efecto desaliento–.

Finalmente, podría darse el caso de que se estuviera obligando al alumnado a ceder sus datos de imagen para poder acceder a un examen –que, además, se presenta a priori con más expectativas de buena nota por la posibilidad de recibir ayudas de diversas fuentes, como vamos a ver inmediatamente–. De nuevo, el alumnado no tendría posibilidad de elección, ya que una de las opciones está muy condicionada.

G. Las TRF pueden generar discriminación por motivos de diversidad funcional

Aun dando por sentado que la interfaz de usuario asociada a un sistema biométrico cumple con la legislación sobre requisitos de accesibilidad aplicable a cualquier sistema electrónico adquirido por la administración pública[16,17], existen en la actualidad interrogantes sobre si estas tecnologías atienden los derechos de las personas con y sin discapacidad (Lee, 2016).

Por ejemplo, en el caso del uso de las TRF por parte de las personas ciegas o con visión limitada, hay estudios (Poh et al., 2016) en los que se describe que las personas con discapacidad visual tienen problemas para tomar "selfies", debido a que un posible mal posicionamiento de la cámara hace que la cara esté borrosa o descentrada. Es necesario considerar que los "selfies" constituyen información clave para algunas TRF. Posibles soluciones a este problema son sistemas de guiado sonoro o háptico para la realización del "selfie", de forma que se asegure que este tiene las características necesarias para que el algoritmo de la TRF funcione, o la implementación de algoritmos que consideren estos aspectos.

Otros sistemas biométricos plantean, por su propia naturaleza, barreras de accesibilidad para grupos específicos de usuarios. Es el caso del reconocimiento de voz, los patrones de pulsación del teclado, reconocimiento de iris, etc. (Blanco-Gonzalo et al., 2018).

La recomendación general para que los derechos humanos queden salvaguardados es que se analicen las diferentes necesidades funcionales de la comunidad que va a hacer uso del sistema y se arbitren soluciones alternativas, ya sean de tipo biométrico o de otro carácter, que aseguren que dichas necesidades quedan razonablemente cubiertas (en el mismo sentido, AEPD, 2020).

H. Las TRF no garantizan la autoría ni la ausencia de utilización de medios fraudulentos en la realización de las pruebas online

El mero reconocimiento facial no supone la limpieza en la realización de los exámenes. Ello es así al menos en dos ámbitos, el de la posibilidad de intervención de terceras personas y el de la utilización de materiales no permitidos para el desarrollo de las pruebas.

En cuanto al primero de ambos aspectos, habría que garantizar, para empezar, que lo mostrado en la pantalla no pueda derivarse hacia otros periféricos de forma que otra persona pueda leer el examen y prestar ayuda –una simple fotografía bastaría para conseguir el efecto no deseado–.

En cuanto a la utilización de materiales no permitidos, las limitaciones de las cámaras impiden el control de los medios con los que cuenta el examinando en el momento de realización de la prueba, poniendo en entredicho el auténtico nivel de sus conocimientos.

Todo ello deriva en una nueva ruptura del principio de igualdad, puesto que quienes se examinan presencialmente cuentan con tribunales que se encargan de su supervisión in situ, pudiéndose derivar responsabilidad disciplinaria en el caso de infracciones del reglamento de pruebas presenciales.

Pero, además, en el momento actual, la utilización masiva de las TRF en la realización de los exámenes supondría la puesta en cuestión del mantenimiento de los estándares de calidad en los que se basa el éxito de la universidad, particularmente la semipresencial. Las pruebas presenciales y el sistema de valija virtual son, sin lugar a duda, dos de los aspectos más reconocidos y reconocibles de nuestra universidad, por su fiabilidad y su alto nivel tecnológico. El desarrollo de un sistema online que trasladara las características del mismo al ámbito virtual con garantías para la privacidad de los estudiantes aparecía como una respuesta adecuada a la situación provocada por la pandemia.

Preguntas acerca del uso del reconocimiento facial en los exámenes universitarios

Sabiendo que aún no existe un consenso acerca de la solución software que podría implementar los exámenes *online*, es importante hacerse algunas preguntas acerca de la misma.

¿Se trataría de una aplicación descargable? ¿Se conectaría el estudiante al campus virtual y allí se desplegaría un interfaz web a la aplicación? ¿Se grabaría o almacenaría toda la sesión del examen? ¿Respecto a qué se realizaría la identificación biométrica? ¿Se haría respecto a las fotos que dieron los estudiantes en su matrícula? ¿Podrían garantizarse unas tasas de éxito suficiente con esas imágenes? ¿Cómo se aseguraría que los datos biométricos iniciales –en caso de que no sean los de la fotografía de sus carnés– son los del alumnado?

RIED. Revista Iberoamericana de Educación a Distancia (2022), 25(1), pp. 261-277.
DOI: https://doi.org/10.5944/ried.25.1.31533 – ISSN: 1138-2783 – E-ISSN: 1390-3306

Es seguro que habría un número de casos no despreciable en los que, incluso con el consentimiento del o de la estudiante, el sistema va a fallar y habría que dar respuesta en un plazo de minutos. De lo contrario, el examen empezaría para unos a una hora y para otros después, incluso mucho después, con lo que eso implica. Pero, lo que es aún más grave, sería probable que estos fallos no fueran aleatorios, sino que, desgraciadamente, estén sesgados. Es posible concebir sesgos perversos como que ocurran más en casos de estudiantes con pocos recursos o que dispongan de equipos informáticos anticuados o baratos e incluso con determinadas características físicas.

CONCLUSIONES

Cualquier institución universitaria, a la hora de plantear soluciones no presenciales para los exámenes, debe regirse siempre por el principio de precaución. Esto implica, respecto a las tecnologías de reconocimiento facial, que debería poder responder a todas las cuestiones que se plantean en este artículo antes de tomar la decisión de adoptarlas.

Además, como hemos argumentado, a la hora de replicar en el ámbito virtual la experiencia de los exámenes presenciales, el uso de tecnologías de reconocimiento facial no es ni mucho menos imprescindible ni está justificado por su efectividad. Lo cierto es que existen otros medios menos arriesgados y más eficaces, como el acompañamiento remoto por parte de los equipos docentes a través de fotografías o vídeos en directo del alumnado o los elementos que dificultan el plagio (aleatorización de preguntas y respuestas, bancos de preguntas amplios que garantizan que dos estudiantes no tendrán el mismo examen, ajuste de los tiempos por pregunta, presentación secuencial de las preguntas, etc.).

La experiencia en la UNED, que finalmente desarrolló para sus exámenes durante las restricciones de movimiento causadas por la COVID-19 un sistema que evita el uso de tecnologías de reconocimiento facial al tiempo que replica en lo posible la experiencia habitual del alumnado en los exámenes presenciales, permite ser optimistas a este respecto. Como se expondrá con detalle en un futuro trabajo en preparación, este caso demuestra que es perfectamente posible realizar un gran número de exámenes (hasta la fecha más de un millón doscientos mil exámenes) con un índice de incidencias igual o menor al que se registra habitualmente en las pruebas presenciales y un alto grado de satisfacción entre el alumnado.

NOTAS

1. https://www.euractiv.com/section/digital/news/leak-commission-considers-facial-recognition-ban-in-ai-white-paper/
2. https://www.banfacialrecognition.com/map/
3. https://www.cbsnews.com/news/facial-recognition-technology-future-check-and-balances/?ftag=CNM-00-10aab7e&linkId=68609640

4. https://www.vice.com/en_us/article/z3bgpj/heres-why-im-campaigning-against-facial-recognition-in-schools
5. https://participa.uned.es
6. Vicerrectorado Adjunto de Gestión Inteligente de Datos y Recursos. *Consideraciones éticas en torno al uso de tecnologías basadas en datos masivos***.** UNED, 2019. https://participa.uned.es/uploads/decidim/attachment/file/183/ConsideracionesEticas_v1.9.pdf
7. Un análisis más extenso de los problemas de las TRF puede verse en Ferguson (2021); en nuestro país, más brevemente, AEPD (2020).
8. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales. *Boletín Oficial del Estado*. Madrid, 6 de diciembre de 2018, pp. 119788 - 119857. https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673
9. 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. *Diario Oficial de la Unión Europea*, 4 de mayo de 2016, L 119/2-89. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32016R0679
10. https://www.article19.org/resources/un-resolution-affirms-surveillance-that-is-not-necessary-or-proportionate-is-against-the-right-to-privacy/
11. Pueden verse amplias referencias al principio de proporcionalidad, entre la jurisprudencia más reciente, en STC 148/2021, de 14 de julio y los votos particulares a la misma, respecto a la constitucionalidad de la declaración del estado de alarma en España con ocasión de la pandemia producida por la COVID-19. Disponible en https://www.boe.es/buscar/doc.php?id=BOE-A-2021-13032
    Sobre la relación entre principio de proporcionalidad y derechos fundamentales, imprescindibles: Bernal (2014) y, todavía hoy, Günther (1983).
12. Cuestiona también la necesidad de la utilización de las TRF, salvo supuestos muy concretos, por la existencia de medidas alternativas el Gabinete Jurídico de la Agencia España de Protección de datos); véase su informe 0036/2020 (abril de 2020); igualmente, rechazando su aplicación con carácter general, García Peñalvo et al. (2020).
13. https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28
14. https://www.wired.com/story/best-algorithms-struggle-recognize-black-faces-equally/
15. https://theconversation.com/automation-can-leave-us-complacent-and-that-can-have-dangerous-consequences-62429
16. Directiva (UE) 2019/882 del Parlamento Europeo y del Consejo, de 17 de abril de 2019, sobre los requisitos de accesibilidad de los productos y servicios. *Diario Oficial de la Unión Europea*, 7 de junio de 2019, L 151/70-115. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=uriserv:OJ.L_.2019.151.01.0070.01.SPA&toc=OJ:L:2019:151:TOC
17. Real Decreto 1112/2018, de 7 de septiembre, sobre accesibilidad de los sitios web y aplicaciones para dispositivos móviles del sector público. *Boletín Oficial del Estado*. Madrid, 19 de septiembre de 2018, pp. 90533 a 90549.

REFERENCIAS

Agencia Española de Protección de Datos (AEPD) (2020). *Informe 0036/2020*. Gabinete Jurídico. https://www.aepd.es/es/documento/2020-0036.pdf

Andrejevic, M., y Selwyn, N. (2019). Facial recognition technology in schools: critical questions and concerns. *Learning, Media and Technology, 45:2,* 115-128. https://doi.org/10.1080/17439884.2020.1686014

Apampa, K., Wills, G., y Argles, D. (2010). An Approach to Presence Verification in Summative e-Assessment Security. *2010 International Conference on Information Society,* (pp. 647–651). IEEE. https://doi.org/10.1109/i-Society16502.2010.6018836

Aznarte, J. L. (2020). Consideraciones éticas en torno al uso de tecnologías basadas en datos masivos en la UNED. *RIED. Revista Iberoamericana de Educación a Distancia, 23*(2). https://doi.org/10.5944/ried.23.2.26590

Aznarte, J. L., y Lacruz, J. M. (10 de febrero de 2021). Vigilancia automática de exámenes: un gran hermano torpe y peligroso. *El País*. https://elpais.com/educacion/2021-02-10/vigilancia-automatica-de-examenes-un-gran-hermano-torpe-y-peligroso.html

Bernal, C. (2014). *El principio de proporcionalidad y los derechos fundamentales*, 4ª ed., Universidad Externado de Colombia.

Blanco-Gonzalo, R., Lunerti, C., Sanchez Reillo, R., y Guest, R. M. (2018), Biometrics: Accessibility challenge or opportunity? *Plos One*. https://doi.org/10.1371/journal.pone.0196372

Crawford, K., Dobbe, R., Dryer, T., Fried, G., Green, B., Kaziunas, E., Kak, A., Mathur, V., McElroy, E., Nill Sánchez, A., Raji, D., Rankin, J. L., Richardson, R., Schultz, J., Myers West, S., y Whittaker, M. (2019). *AI Now 2019 Report*. New York: AI Now Institute. https://ainowinstitute.org/AI_Now_2019_Report.html.

Dewan, M., Akber, A., Murshed, M., y Lin, F. (2019). Engagement Detection in Online Learning*:* A Review. *Smart Learning Environments, 6*(1). https://doi.org/10.1186/s40561-018-0080-z

Doffman, Z. (2018). Why facial recognition in schools seems to be an aimless recipe for disaster. *Forbes,* 7th November. https://www.forbes.com/sites/zakdoffman/2018/11/07/why-facial-recognition-in-schools-seems-to-be-an-aimless-recipefordisaster/#7abc4f01a83a

Ferguson, A. G. (2021). Facial Recognition and the Fourth Amendment. *Minnesota Law Review*. https://minnesotalawreview.org/article/facial-recognition-and-the-fourth-amendment/

García-Peñalvo, F. J., Corell, A., Abella-García, V., y Grande M. (2020). La evaluación online en la educación superior en tiempos de la COVID-19. *Education in the Knowledge Society, 21*. https://doi.org/10.14201/eks.23086

Günther, H. L. (1983). *Strafrechtswidrigkeit und Strafunrechtsausschluss: Studien zur Rechtswidrigkeit als Straftatmerkmal un zur Funktion der Rechtfertigungsgründ im Strafrecht*. Carl Heymanns Verlag.

Hernández, J., Ortiz, A., Andaverde, J., y Burlak, G. (2008). Biometrics in Online Assessments: A Study Case in High School Students. *18th International Conference on Electronics, Communications and Computers (conielecomp 2008),* (pp. 111-116). IEEE. https://doi.org/10.1109/CONIELECOMP.2008.36

Izquierdo, M. (2020). La utilización policial de los sistemas de reconocimiento facial automático. Comentario a la sentencia del Alto Tribunal de Justicia de Inglaterra y Gales de 4 de septiembre de 2019. *IUS ET VERITAS*, 60. https://doi.org./10.18800/iusetveritas.202001.004

Lascuraín, J. A. (2020). *El principio de proporcionalidad penal: cinco retos (I)*. https://almacendederecho.org/el-principio-de-proporcionalidad-penal-cinco-retos-i

Lee, T. (2016). Biometrics and disability rights: legal compliance in biometric identification programs. *Journal of Law, Technology & Policy*. http://illinoisjltp.com/journal/wp-content/uploads/2016/11/Lee.pdf

Martínez, R. (2020). Tecnología de verificación de identidad y control en exámenes online. *Revista de Educación y Derecho*, *22*. https://doi.org/10.1344/REYD2020.22.32357

Montag, L., Mcleod, R., De Mets, L., Gauld, M., Rodger, F., y Petka, M. (2021). *The rise and rise of biometrics mass surveillance in the EU. A legal analysis of biometrics mass surveillance practices in Germany, The Netherlands, and Poland*. EDRi. http://edri.org/wp-content/uploads/2021/07/EDRI_RISE_REPORT.pdf

Montgomery, J., y Marais, A. (2014). *Educational Content Access Control System*. U.S. Patent Application 14/212,069, filed September 18, 2014.

Navarro, I. (2010). El principio de proporcionalidad en sentido estricto: ¿principio de proporcionalidad entre el delito y la pena o balance global de costes y beneficios? *InDret Penal*. https://indret.com/wp-content/themes/indret/pdf/724.pdf

Perelló, I. (1997). El principio de proporcionalidad y la jurisprudencia constitucional. *Jueces para la Democracia*. https://dialnet.unirioja.es/servlet/articulo?codigo=174691

Poh, N., Blanco-Gonzalo, R., Wong, R., y Sánchez Reillo, R. (2016), Blind subjects faces database. *IET*. https://doi.org/10.1049/iet-bmt.2015.0016

Roca, E. (2013). Los principios de razonabilidad y proporcionalidad en la jurisprudencia constitucional española. *Reunión de Tribunales Constitucionales de Italia, Portugal y España*. https://www.tribunalconstitucional.es/es/trilateral/documentosreuniones/37/ponencia%20espa%C3%91a%202013.pdf

Rodicio-García, M., Ríos-de-Deus, M., Mosquera-González, M., y Penado Abilleira, M. (2020). La Brecha Digital en Estudiantes Españoles ante la Crisis de la Covid-19. *Revista Internacional de Educación para la Justicia Social*, *9*(3). https://doi.org/10.15366/riejs2020.9.3.006

Stark, L. (2019). *Facial Recognition is the Plutonium of AI*. XRDS - Crosswords (ACM), April 2019. https://doi.org/10.1145/3313129

Valera, J., Valera, J., y Gelogo, Y. (2015). A Review on Facial Recognition for Online Learning Authentication. *8th International Conference on Bio-Science and Bio-Technology (BSBT),* Jeju, 16-19. https://doi.org/10.1109/BSBT.2015.15

PERFIL ACADÉMICO Y PROFESIONAL DE LOS AUTORES

José L. Aznarte. Profesor titular en el departamento de Inteligencia Artificial de la UNED, y vicerrector adjunto de gestión inteligente de datos y recursos. Fue investigador post-doc en la universidad Mines ParisTECH (Francia). Recibió un contrato "Ramón y Cajal" (2013) y obtuvo la certificación I3 (2018). Es autor de más de 35 publicaciones en revistas de prestigio y tiene un índice h de 16. Sus intereses de investigación giran en torno a la predicción de series temporales y algunas de sus aplicaciones menos relacionadas con asuntos económicos, como la predicción de

la calidad del aire, el tráfico o la propagación de epidemias. Coordina el desarrollo de SOCAIRE, el sistema predictivo que permite la anticipación de la activación del protocolo de NO2 del Ayuntamiento de Madrid y es director de la Cátedra EMT/ UNED de Calidad del Aire y Movilidad Sostenible. https://orcid.org/0000-0002-1636-244X
E-mail: jlaznarte@dia.uned.es

DIRECCIÓN DEL AUTOR
Departamento de Inteligencia Artificial
Escuela Técnica Superior de Ingeniería Informática
Calle Juan del Rosal, 16
28040 Madrid (España)

Mariano Melendo Pardos. Profesor titular de universidad. Política criminal y sistema del Derecho Penal; racionalidad legislativa, teoría de la legislación y argumentación jurídica; la proyección de los derechos fundamentales en el derecho disciplinario; el reflejo de los principios básicos del derecho penal en la potestad sancionadora de la Administración.
E-mail: mmelendo@der.uned.es

Juan Manuel Lacruz López. Profesor titular de Universidad. Teoría jurídica del delito; Política Criminal; regulación penal de los movimientos migratorios; trata de seres humanos; tratamiento penal de la discriminación a los ciudadanos extranjeros; Derecho Penal Juvenil; protección penal de las administraciones públicas; delito fiscal.
E-mail: jlacruz@der.uned.es

DIRECCIÓN DE LOS AUTORES
Departamento de Derecho penal y Criminología
Facultad de Derecho UNED
Calle Obispo Trejo, 2, 3ª planta
28040 Madrid (España)

Fecha de recepción del artículo: 16/09/2021
Fecha de aceptación del artículo: 14/10/2021
Fecha de aprobación para maquetación: 26/10/2021