avances en Supervisión educativa
Revista de la Asociación de Inspectores de Educación de España

Inteligencia artificial y protección de datos en el ámbito de la educación en España

/

Artificial Intelligence and Data Protection in Education in Spain

Francisco Javier Galicia Mangas.

Profesor de enseñanza secundaria del Gobierno de Aragón. Doctor en Derecho, máster en Derecho de la Administración pública, y profesor asociado de la Facultad de Derecho de la Universidad de Zaragoza[*].

DOI: https://doi.org/10.23824/ase.v0i44.1019

Resumen

Objetivos: verificar el grado de cumplimiento de la normativa de protección de datos por parte de los sistemas de IA utilizados en el ámbito educativo. Metodología: la propia de las ciencias sociales y jurídicas, que parte del estudio de la situación actual y del marco normativo aplicable, para valorar la efectividad de su aplicación y proponer medidas de garantía de los derechos. Resultados: se observan dificultades en la protección de datos personales, derivadas de un avance tecnológico mucho más apresurado que el normativo de garantía de los derechos protegidos. Conclusiones: Los sistemas de IA utilizados en el ámbito educativo deben cumplir las estrictas normas vigentes en el ámbito europeo en materia de protección de datos personales, pero se detectan serias dificultades prácticas para garantizar de manera efectiva dicho cumplimiento.

Palabras clave: Educación; inteligencia artificial; protección de datos.

[*] Contacto: fgalicia@unizar.es

Abstract

Objectives: to verify the degree of compliance with data protection regulations by Artificial Intelligence systems used in education. Methodology: that of the social and legal sciences, based on a study of the current situation and the applicable regulatory framework in order to assess the effectiveness of its application and propose measures to guarantee rights. Outcomes: there are difficulties in the protection of personal data, due to a technological advance much faster than the normative granting of protected rights. Conclusions: AI systems used in education must comply with the strict European rules on personal data protection, but there are serious practical difficulties to ensure effective compliance.

Key words: Education; artificial Intelligence; data protection.

Índice

4. Principales riesgos y desafíos en protección de datos.
   4.1 Datos de menores.
   4.2 Decisiones automatizadas y perfilado.
   4.3 Transferencias internacionales de datos.
   4.4 Sesgos algorítmicos y discriminación.
   4.5 Seguridad y brechas de datos.
5. Jurisprudencia y resoluciones relevantes.
   5.1 Jurisprudencia española.
   5.2 Jurisprudencia europea (TJUE).
   5.3 Resoluciones internacionales.
6. Medidas legales, buenas prácticas y estrategias de cumplimiento en materia de protección de datos.
   6.1 Delegado de Protección de Datos (DPD).
   6.2 Evaluaciones de Impacto en Protección de Datos (EIPD).
   6.3 Políticas de consentimiento informado.
   6.4 Privacidad desde el diseño y protección de datos por defecto.
   6.5 Formación del profesorado y concienciación.
   6.6 Implementación de buenas prácticas.
7. Conclusiones.

Normativa básica de referencia

Otros documentos

Bibliografía.

1. Introducción

En los últimos años, la inteligencia artificial (IA) se ha consolidado como una de las tecnologías más influyentes en todos los ámbitos de la sociedad. En el contexto educativo, su impacto es especialmente relevante, ya que afecta de forma directa a la enseñanza, al aprendizaje, a la organización de los centros y a la protección de los derechos fundamentales de los alumnos.

La incorporación de herramientas de IA en las aulas plantea retos inéditos en materia de protección de datos[1]. Estos retos son particularmente sensibles, dado que el sistema educativo trabaja con datos de menores de edad, categoría especialmente protegida por el Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD).

El presente artículo tiene como finalidad analizar, desde una perspectiva académica y jurídica, los retos que puede plantear para la protección de datos personales, en especial de menores de edad, el uso de la inteligencia artificial en el ámbito de la educación en España, ofreciendo una panorámica completa que abarque:

- El marco normativo español y europeo aplicable, en especial la regulación de la IA en Europa (*AI Act*) y su impacto en el sistema educativo.
- Los principales usos y aplicaciones de la IA en la educación.
- Los riesgos y desafíos jurídicos, éticos y sociales.
- La jurisprudencia y resoluciones relevantes.
- Buenas prácticas y recomendaciones de cumplimiento.

El enfoque se dirige a un público amplio, que incluye a docentes, equipos directivos, inspectores de educación, juristas, responsables de protección de datos, y a la sociedad en general. El estudio se centra principalmente en el ámbito de la educación primaria y secundaria, aunque también podrían hacerse extensivas sus

[1] Recientes estudios plantean que las inversiones actuales en IA generativa-razonadora aún no son rentables, al menos a la velocidad de expansión actual, y quizás no lo sean antes de 2029. Subsisten gracias a apoyos externos, fuertes inversiones con perspectiva de futuro, o a los recursos de otros servicios ya lucrativos como el almacenamiento en la nube, pero lo que desde luego está claro es que una fuente muy destacada de recursos para financiar este desarrollo, parte del elevado precio que se está pagando por los datos obtenidos, principalmente de los usuarios de la red (véase artículo publicado en el diario Heraldo de Aragón por Gonzalo Castro Marquina, con el título “Las IA de Newcomen”, el martes 26 de agosto de 2025, p. 15). En el mismo sentido véanse los razonamientos sobre inversiones en proyectos educativos de educación superior y gastos de entrenamiento y mantenimiento de modelos como OpenAI y ChatGPT en P. Gallego Rodríguez (pp. 196 y 197).

apreciaciones en buena medida al ámbito docente universitario. El lenguaje utilizado será técnico, pero accesible, combinando doctrina, normativa y ejemplos prácticos.

2. Marco normativo europeo y español de referencia

Este epígrafe, a modo de introducción, pretende ofrecer una visión general del marco jurídico vigente en España y la Unión Europea sobre protección de datos en el ámbito educativo[2], con el fin de contextualizar el uso de la IA en la actividad docente.

2.1 Reglamento General de Protección de Datos de la UE (RGPD)

Desde su entrada en vigor el 25 de mayo de 2018, el Reglamento (UE) 2016/679, de 27 de abril de 2016[3], es la norma básica que rige en todo el territorio de la Unión Europea (UE). Dicho Reglamento garantiza, como a toda la ciudadanía en general, una serie de derechos básicos aplicables al alumnado, personal docente y sus familias, entre los cuales cabe destacar los de transparencia (art. 12), información (arts. 13 y 14), acceso (art. 15), rectificación (art. 16) supresión o derecho al olvido (art. 17), limitación del tratamiento (art. 18), portabilidad de datos (art. 20), y oposición (art. 21).

Cierto es que es el RGPD no contiene ninguna referencia específica relativa a la IA[4], pero no por ello deja de ser aplicable su regulación a esta evolución de la técnica. No en vano, la IA basa su funcionamiento en el uso de gran cantidad de datos, muchos de ellos personales, dado que se sirve en su operativa del conocido como *big data*. Ello implica, necesariamente, que el RGPD sirva como regulación de referencia de la IA, de la misma manera que cualquier otro instrumento que procese o utilice datos personales en el contexto europeo.

De especial trascendencia en esta norma, para su aplicación en el ámbito educativo, es la definición y regulación de las figuras del responsable del tratamiento de datos, del encargado/a, y del delegado/a de protección de datos.

[2] Para un estudio más detallado de esta cuestión puede verse F. J. Galicia Mangas (2019).
[3] Nos referimos al 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, más conocido como Reglamento General de Protección de Datos (RGPD).
[4] Como bien sabemos, la celeridad de los avances tecnológicos suele ser muy superior a la de los avances normativos, que siempre parecen ir un paso por detrás.

Responsable del tratamiento es, según el art. 4.7 del RGPD "la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento"[5]. Llevado a la práctica esto supone que, en el ámbito de la educación, las responsables del tratamiento de datos son las Administraciones educativas, en el caso de los centros públicos, y las entidades titulares, en el caso de los centros privados y concertados.

Encargado/a del tratamiento es, conforme a lo dispuesto en el art. 4.8 del RGPD "la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento".

Aunque, en apariencia, esto nos podría llevar a concluir que encargado del tratamiento en los centros docentes es el personal, funcionario o laboral, que presta servicio en los mismos, la Agencia Española de Protección de Datos (AEPD), ha matizado que no ostentan tal condición las personas físicas que tengan acceso a los datos personales en su calidad de empleados del centro o de la Administración educativa, lo cual excluye tanto al profesorado y equipos directivos, como al personal de administración y servicios, pero no a otros sujetos de los que los centros educativos se sirven para prestar servicios, y que no se integran en su organización (ej. servicio de transporte, comedor escolar, actividades extraescolares, u otros).

Pero, sin lugar a duda, la novedad más relevante ha sido la incorporación de la figura del delegado de protección de datos (arts. 37 a 39 RGPD).

De forma muy sintética, y sin perjuicio de una posterior explicación más detallada, podemos decir que sus misiones principales giran alrededor del asesoramiento, coordinación y control del cumplimiento en materia de protección de datos.

Esta figura es además, de conformidad con lo dispuesto en el art. 37.1.a del RGPD, obligatoria en aquellos supuestos en los que "el tratamiento lo lleve a cabo una autoridad u organismo público".

[5] La Agencia Española de Protección de Datos (AEPD) considera, en aclaración o matización de este precepto, que responsable del tratamiento es la persona física o jurídica, pública o privada, que decide sobre la finalidad, contenido y uso del mismo, bien por decisión directa o porque así le viene impuesto por una norma legal.

Por último, advertir que no siempre resulta sencillo establecer cuándo un sistema de IA, a lo largo de su ciclo de vida, trata o no datos personales[6]. Ahora bien, parece evidente que si no se produce ese tratamiento no resulta aplicable el RGPD. En caso contrario, es decir, en aquellos supuestos en los que se realiza el tratamiento de datos personales (ej. si se elaboran perfiles personales o se toman decisiones basadas en dichos perfiles), dichas actuaciones del sistema IA quedarán sujetas al RGPD.

2.2 Reglamento Europeo de Inteligencia Artificial (RIA)

Nos referimos, en este caso, al Reglamento (UE) 2024/1689, de 13 de junio de 2024[7], por el que se establecen normas armonizadas en materia de inteligencia artificial, más conocido de forma abreviada como Reglamento de Inteligencia Artificial (RIA)[8] o por sus siglas en inglés como *EU AI Act*.

El propio Reglamento define la IA en su art. 3 como,

> un sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales.

[6] El tratamiento de datos personales puede abarcar las siguientes etapas del ciclo de vida de la IA: fase de entrenamiento, validación, despliegue, explotación, y retirada. Hay que recordar asimismo que no todas las soluciones IA tratan datos personales ni afectan a personas físicas, como por ejemplo las que controlan la calidad de productos industriales. Para mayor detalle, véase AEPD, Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción (pp. 12 a 14).

[7] Sobre la génesis, desarrollo y dificultades de elaboración de este Reglamento, así como sobre el impacto que puede tener esta norma a nivel global véase C. Artigas Oliveras (2024). Debe dejarse constancia asimismo de las habituales reticencias de las empresas del sector hacia una regulación que pueda limitar su desarrollo y beneficio, circunstancias estas últimas que dependen en buena medida de "un modelo de desarrollo tecnológico con los datos e información en manos privadas y concentrado en un puñado de grandes empresas tecnológicas" (Artigas Oliveras, 2024, p. 22).

[8] Conforme a lo establecido en su art. 113 este Reglamento entró en vigor el 1 de agosto de 2024, a los 20 días de su publicación en el DOUE (12 de julio de 2024). No obstante, dicho art. 113 establece asimismo que, con carácter general, será aplicable a partir del 2 de agosto de 2026, con las siguientes excepciones:
"a) los capítulos I y II serán aplicables a partir del 2 de febrero de 2025;
b) el capítulo III, sección 4, el capítulo V, el capítulo VII y el capítulo XII y el artículo 78 serán aplicables a partir del 2 de agosto de 2025, a excepción del artículo 101;
c) el artículo 6, apartado 1, y las obligaciones correspondientes del presente Reglamento serán aplicables a partir del 2 de agosto de 2027".

Su carácter de Reglamento UE, como sucede igualmente en el caso del RGPD, determina que sea obligatorio en todos sus elementos, y directamente aplicable en cada Estado miembro, lo que marca su extraordinaria trascendencia.

No obstante, y como bien advierte Razquin Lizarraga (2024, p. 177), es preciso tomar en consideración que el RIA regula solamente "aquellos sistemas de IA que tengan riesgo inadmisible o elevado, dejando fuera de su regulación el resto de los sistemas de IA".

Así pues, podemos concluir que, los sistemas de IA de riesgo limitado están permitidos, aunque sujetos a obligaciones de transparencia e información[9], y los de riesgo bajo o nulo quedan al margen de la aplicación del RIA, si bien los operadores pueden vincularse en este último supuesto, de forma voluntaria, al cumplimiento de códigos de conducta o de buenas prácticas.

El valor e importancia de la IA queda reflejado desde los primeros párrafos, en los que se destaca la gran cantidad de beneficios y ventajas que puede generar desde el punto de vista social, en general, y de la educación y formación en particular (Considerando 4).

Pero, igualmente se deja constancia de sus peligros, lo que provoca que, tomando en consideración los efectos que pueden derivar para los derechos fundamentales de las personas, la IA pueda ser clasificada como un sistema de alto riesgo en relación con la protección de datos de carácter personal en general (Considerandos 9, 10, 48 y 69, entre otros), y para algunos aspectos relativos al ejercicio del derecho a la educación, en particular[10] (Considerandos 48 y 56).

Según lo establecido en el Considerando 56, "el despliegue de sistemas de IA en el ámbito educativo es importante para fomentar una educación y formación digitales de alta calidad (…)".

[9] La regulación de los sistemas de IA de alto riesgo en el RIA es extensa, y comprende todo el capítulo III de la norma (arts. 6 a 49), el anexo III, y citas y referencias regulatorias diversas a lo largo del resto del contenido de misma. No obstante, con fecha de 19 de noviembre de 2025 la Comisión Europea ha formulado un conjunto de propuestas para simplificar la normativa reguladora de la IA, entre las cuales hay que destacar una flexibilización en el marco de protección de datos en el sector digital y, sobre todo, el aplazamiento de la aplicación durante 16 meses, de las reglas regulatorias de la IA de alto riesgo, es decir, hasta diciembre de 2027.

[10] Sobre la consideración de la IA en el ámbito de la educación como sistema de alto riesgo y sus consecuencias, véase M. M. Razquin Lizarraga (2024, p. 209)

Sin embargo, como se decía con anterioridad, su uso no está exento de dificultades, en especial en aquellas actuaciones que conllevan procesos de acceso, admisión o distribución de personas en el sistema, centros o programas educativos; las que suponen evaluación de los resultados de aprendizaje o del nivel educativo, o las que supervisan y detectan comportamientos prohibidos de los estudiantes durante el desarrollo de pruebas evaluables.

Todas estas actuaciones de riesgo[11] presentan un elemento común, a saber, la posible vulneración del derecho a la educación y del derecho a no sufrir discriminación.

Por ello, el anexo III del Reglamento, al reseñar los Sistemas de IA de alto riesgo a que se refiere el apartado 2 del artículo 6, establece que:

> Los sistemas de IA de alto riesgo con arreglo al artículo 6, apartado 2, son los sistemas de IA que formen parte de cualquiera de los ámbitos siguientes:
>
> 3. Educación y formación profesional:
>
> a) Sistemas de IA destinados a ser utilizados para determinar el acceso o la admisión de personas físicas a centros educativos y de formación profesional a todos los niveles o para distribuir a las personas físicas entre dichos centros.
>
> b) Sistemas de IA destinados a ser utilizados para evaluar los resultados del aprendizaje, también cuando dichos resultados se utilicen para orientar el proceso de aprendizaje de las personas físicas en centros educativos y de formación profesional a todos los niveles.
>
> c) Sistemas de IA destinados a ser utilizados para evaluar el nivel de educación adecuado que recibirá una persona o al que podrá acceder, en el contexto de los centros educativos y de formación profesional o dentro de estos a todos los niveles
>
> d) Sistemas de IA destinados a ser utilizados para el seguimiento y la detección de comportamientos prohibidos por parte de los estudiantes durante

[11] El art. 3.2 del RIA define el riesgo como “la combinación de la probabilidad de que se produzca un perjuicio y la gravedad de dicho perjuicio”.

los exámenes en el contexto de los centros educativos y de formación profesional o dentro de estos a todos los niveles.

Especialmente destacable es pues el conjunto de medidas adoptadas para que estos sistemas de IA de alto riesgo cumplan las medidas de protección necesarias, así como la determinación de los sujetos responsables.

De todo ello se da buena cuenta en la Sección 2 del capítulo III (arts. 8 a 15), dedicada a los requisitos de los sistemas de IA de alto riesgo[12], y en la sección 3 del mismo capítulo (arts. 16 a 27), que establece las obligaciones de los proveedores y responsables del despliegue de sistemas de IA de alto riesgo y de otras partes.

De especial relevancia es también el art. 10 de la norma, dada la estrecha conexión existente entre los sistemas de IA y sus técnicas de entrenamiento con datos, en especial si son datos personales, reglas que tienen como fin último, impedir que se produzcan sesgos que afecten a los derechos fundamentales de las personas, o den lugar a discriminación, específicamente cuando los datos recabados puedan ser utilizados en futuras operaciones de toma de decisiones. Entre estas reglas de protección figura, asimismo, el establecimiento, como garantía, de la posibilidad de supervisión humana durante su periodo de uso (art. 14).

Por último, para cerrar este apartado dedicado a la regulación de la IA en la UE, advertir que no disponemos en nuestro país de una norma propia con rango de Ley que regule esta cuestión y aplicable en todo el territorio nacional.

No obstante, dejar al menos constancia de la existencia del Real Decreto 729/2023, de 22 de agosto, por el que se aprueba el Estatuto de la Agencia Española de Supervisión de Inteligencia Artificial -AESIA- (BOE de 2 de septiembre de 2023), organismo de Derecho público que tiene por objeto y fin básico la supervisión e inspección del desarrollo y despliegue de la IA en nuestro país (art. 4).

[12] Véase además sobre el particular Razquin Lizarraga (2024, pp. 217 a 228): Dichos requisitos son los siguientes: 1) implantación de un sistema de gestión de riesgos, 2) realización de prácticas de gobernanza de datos para el caso de entrenamiento de modelos de IA, 3) elaboración de la documentación técnica del sistema de IA, 4) trazabilidad asegurada mediante un registro automático de eventos, 5) transparencia y comunicación de información a los responsables del despliegue, 6) vigilancia humana, y 7) nivel adecuado de precisión, solidez y ciberseguridad.

2.3 Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDP)

La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales[13] (en adelante LOPDP), en vigor en España desde el 7 de diciembre del mismo año, es la norma de referencia en nuestro país para la garantía de los derechos digitales, y sirvió para adaptar el Ordenamiento jurídico español al RGPD[14].

Esta norma, presenta a su vez una íntima conexión con el art. 18.4 de la Constitución, al que posteriormente se hará referencia, y sirvió asimismo para introducir una modificación en la Ley Orgánica 2/2006, de 3 de mayo, de Educación (LOE), modificación estrechamente relacionada con la capacitación del alumnado en el correcto uso de los medios digitales, y en el respeto de la intimidad tanto individual como colectiva, cuestiones muy relevantes, dado el amplio uso que hacemos de las nuevas tecnologías en los centros docentes[15].

Al igual que ya se advirtió en relación con el RGPD, en la LOPDP no encontraremos tampoco ninguna referencia explícita a los sistemas de IA, pero su regulación resulta también aplicable[16].

Complementando lo dispuesto y ya comentado en relación con el RGPD, cabe decir ahora que la LOPDP establece una profusa regulación de las figuras del responsable, del encargado y del delegado de protección de datos, regulación que se extiende a lo largo de todo el articulado de forma directa o indirecta.

---

[13] Hasta la entrada en vigor del futuro Reglamento de Desarrollo de la Ley Orgánica 3/2018 (LOPDP) sigue vigente el Real Decreto 1720/2007, de 21 de diciembre, de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos Personales, en todo aquello que no se oponga a lo establecido en el RGPD y a la nueva LOPDP de 2018.

[14] En relación con las novedades más relevantes incorporadas por esta norma y por el RGPD para la protección de datos personales en los centros docentes, con los derechos y principios de actuación en la materia, datos especialmente protegidos y su regulación, véase F. J. Galicia Mangas (2019, pp. 4 a 18).

[15] Así, en su DF 10ª, la LOPDP determina la inclusión de una nueva letra "l" en el apdo. 1 del art. 2 de la LOE, que establece como finalidad del sistema educativo "la capacitación para garantizar la plena inserción del alumnado en la sociedad digital y el aprendizaje de un uso seguro de los medios digitales y respetuoso con la dignidad humana, los valores constitucionales, los derechos fundamentales y, particularmente, con el respeto y la garantía de la intimidad individual y colectiva".

[16] La primera norma de rango legal en España que hizo mención expresa de la IA fue la Ley15/2022, de 12 de julio, integral para la igualdad de trato y la no discriminación (BOE de 13 de julio de 2022), norma que contiene la primera regulación positiva del uso de la inteligencia artificial por las Administraciones públicas y las empresas en nuestro país, si bien con un carácter más programático o de mera declaración de buenas intenciones (véanse los arts. 3.1, o y 23), que de aplicación real y efectiva.

No obstante, de forma más concreta, podemos citar, dentro del título V de la norma, los arts. 28 y 33, que regulan las obligaciones generales del responsable y encargado del tratamiento, y los arts. 34 a 37 que regulan la figura del delegado de protección de datos.

2.4 Constitución Española (CE) y jurisprudencia constitucional

Pero, si existe un pilar en el cual se apoya en nuestro Ordenamiento jurídico el legítimo derecho a la intimidad, y a la protección de datos personales ese pilar es el art. 18 de la Constitución española de 1978 (CE), en especial en sus nº 1 y 4:

> Artículo 18 CE.
> 1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen (…)
> 4. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

Aunque, en apariencia, el citado precepto no haga referencia expresa a la protección de datos, la jurisprudencia constitucional, ha dejado claro desde el inicio y de forma reiterada[17], que dicha garantía queda incluida o integrada en sus términos.

Pero, la primera sentencia en la que el Tribunal Constitucional (TC) se pronuncia y consagra el derecho a la protección de datos como derecho fundamental, integrado en el art. 18, es en la STC 254/1993, de 20 de julio (BOE de 18 de agosto de 1993).

La clave se encuentra en su FJ 6º, en el que se afirma que,

> (…) nuestra Constitución ha incorporado una nueva garantía constitucional, como forma de respuesta a una nueva forma de amenaza concreta a la dignidad y a los derechos de la persona (…) En el presente caso estamos ante un instituto de garantía de otros derechos, fundamentalmente el honor y la intimidad, pero también de un instituto que es, en sí mismo, un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos, lo que la Constitución llama «la informática».

[17] Pueden verse las SSTC 11/1998, de 13 de enero, (FJ 5); 292/2000, de 30 de septiembre (FJ 5); 96/2012, (FJ 6); 151/2014, de 25 de septiembre, (FJ 7), y 76/2019 (FJ 5º).

Por último, citar como referente en la materia estudiada la STC 292/2000, de 30 de noviembre (BOE de 4 de enero de 2001), en la que se definen con nitidez el concepto y contenido del derecho a la protección de datos personales, y sus diferencias con el derecho a la intimidad. Su FJ 6º se expresa en los siguientes términos:

> 6. (…) el derecho a la intimidad permite excluir ciertos datos de una persona del conocimiento ajeno, (…) es decir, el poder de resguardar su vida privada de una publicidad no querida. El derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos datos. Esta garantía impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías; y también el deber de prevenir los riesgos que puedan derivarse del acceso o divulgación indebidas de dicha información.

Vemos pues, que la doctrina del máximo intérprete de la Constitución no sólo garantiza el poder de control de los ciudadanos sobre sus datos personales, sino que, además, convierte a los poderes públicos, y dentro de los mismos figuran las Administraciones educativas, en garantes de esa información y obligados a prevenir los riesgos derivados del acceso o divulgación de los mismos.

2.5 Ley Orgánica de Educación (LOE)

La Ley Orgánica 2/2006, de 3 de mayo, de Educación hace referencia directa en algunos de sus preceptos a la protección de datos personales del alumnado.

Por un lado, en el art. 111 bis, en relación con el uso de las TIC tanto en la gestión académica y administrativa como en el proceso de enseñanza y aprendizaje, para garantizar el cumplimiento de la normativa sobre privacidad y protección de datos personales.

Por otro, en la DA 23ª, para autorizar a los centros docentes la obtención de los datos personales necesarios para el ejercicio de la función educativa[18], estableciendo incluso el deber de los progenitores, representantes legales y de los propios alumnos,

[18] No conviene perder de vista el hecho de que algunos de los datos necesarios para el desarrollo de la función educativa son altamente sensibles, como por ejemplo los relativos al “origen y ambiente familiar y social, a características o condiciones personales, al desarrollo y resultados de su escolarización, así como a aquellas otras circunstancias cuyo conocimiento sea necesario para la educación y orientación de los alumnos” (DA 23ª.1).

de colaborar para la obtención de dichos datos, a la par que se garantiza su seguridad, confidencialidad y el deber de sigilo profesional.

2.6 Regulación autonómica

Sin lugar a duda, y como viene siendo habitual, nos estamos encontrando con una incorporación mucho más acelerada de la IA en el campo de la educación[19], que de la normativa que la pueda regular.

El panorama es variado, pero, en líneas generales, la regulación autonómica no alcanza todavía el rango necesario para crear derechos y obligaciones estrictos en todos los sujetos intervinientes.

Así, nos encontramos con toda una panoplia de herramientas que abarcan desde las de mayor rango normativo, como sucede en el caso de Galicia con la Ley 2/2025, de 2 de abril, para el desarrollo e impulso de la inteligencia artificial en Galicia (DOG de 4 de abril de 2025), hasta las más comunes y simples orientaciones y recomendaciones para el uso de la IA en los centros educativos, como sucede en el caso de Cataluña[20], o guías para el uso de las inteligencias artificiales en el ámbito educativo, como por ejemplo, en el País Vasco[21] o la publicada por el Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado (INTEF)[22], de ámbito estatal.

En el nivel intermedio, de rango reglamentario, nos encontramos normas como el Decreto 98/2025, de 22 de julio, por el que se regula el uso de la Inteligencia Artificial en la Administración del Principado de Asturias y su sector público (BOPA de 31 de julio de 2025), o con proyectos normativos como la Orden que tiene previsto promulgar La Comunidad Autónoma de Aragón en octubre de 2025[23], con criterios sobre el uso de equipos digitales, y que también abordará la inteligencia artificial, o la Orden por la que se regulará el desarrollo de la estrategia digital en los centros docentes no

[19] Véanse, a título de simple ejemplo, los recientes acuerdos (2025) firmados por la Comunidad de Madrid con Google para el uso de IA en centros docentes públicos (https://www.comunidad.madrid/noticias/2025/06/27/diaz-ayuso-renueva-convenio-google-todos-colegios-publicos-madrilenos-utilicen-herramientas-educativas-basadas-ia) y por el Gobierno de Aragón con Microsoft, para impulsar la Inteligencia Artificial en la Formación Profesional (https://news.microsoft.com/es-es/2025/06/02/gobierno-de-aragon-impulsara-la-inteligencia-artificial-en-la-formacion-profesional-de-la-mano-de-microsoft/).
[20] Véanse en https://projectes.xtec.cat/ia/
[21] Véase en https://www.ehige.eus/es/normativa-digitalizacion/
[22] Véase en https://intef.es/Noticias/guia-sobre-el-uso-de-la-inteligencia-artificial-en-el-ambito-educativo/
[23] Noticia publica en el periódico Heraldo de Aragón de 30 de agosto de 2025 con el título “Aragón limitará el uso de pantallas en las aulas de colegios e institutos en 2026-2027” (p. 3).

universitarios sostenidos con fondos públicos de la región de Murcia[24] y se crea el sello de calidad digital.

Comenzando por la ley gallega, según su art. 1º tiene por objeto "establecer el marco para el diseño, adquisición, implementación y uso de la inteligencia artificial en la Administración general de la Comunidad Autónoma (…) de conformidad con la regulación de la Unión Europea y la normativa básica estatal en esta materia".

Cierto es que no se centra específicamente en la Administración educativa ni tiene referentes distintos de los ya expuestos con anterioridad, es decir, el RGPD, el RIA, o la LOPDP, pero al menos supone un primer paso en el nivel regulatorio de rango superior que permite, como sostiene su propia exposición de motivos (IV) "dar respuesta a los retos que implican este gran cambio y la demanda de seguridad jurídica en el desarrollo y ejercicio de los derechos de la ciudadanía (…)".

Cabe destacar en esta norma, por la conexión establecida entre los sistemas de IA utilizados por la Administración y la protección de datos, lo dispuesto en los siguientes artículos:

- El art. 11, relativo a la seguridad y privacidad, que se remite en cuanto al nivel de protección de datos personales utilizados por la IA a lo establecido en el RGPD, LOPDP y, en particular, a los "principios de licitud, transparencia, lealtad, limitación de la finalidad, minimización de los datos, exactitud, seguridad, limitación del plazo de conservación y responsabilidad proactiva". Dicha seguridad se aplica "en los procesos de diseño, adquisición, implementación y uso de sistemas de inteligencia por parte de la Administración", y garantiza "la integridad, confidencialidad, disponibilidad y autenticidad de los datos e información tratada mediante el establecimiento de las oportunas medidas de seguridad" (…) así como también que "estos sistemas sean seguros y resilientes frente a terceros que intenten explotar sus vulnerabilidades".

[24] Véase la iniciativa normativa publicada en el Portal de Transparencia de la Región de Murcia, sobre el Proyecto de orden para regular el desarrollo de la estrategia digital en los centros docentes no universitarios sostenidos con fondos públicos. Recuperado a partir de https://transparencia.carm.es/-/orden-desarrollo-estrategia-digital-en-los-centros-docentes-no-universitarios?inheritRedirect=true

- El art. 16, que hace referencia a la evaluación del impacto organizativo, económico, social, y medioambiental, así como a la posible afectación de derechos fundamentales para los sistemas de IA de alto riesgo.
- El art. 25, que regula la tutela de los derechos de toda persona en cuya relación con la Administración intervenga un sistema de IA y, en especial, los derechos en materia de protección de datos personales.

Por su parte, el Decreto 98/2025, del Principado de Asturias, incide en la cuestión relativa a la protección de datos en el uso de sistemas de IA por la Administración en los siguientes artículos:

- art. 3: que garantiza el principio de privacidad y protección de datos en todas las fases del proceso vital de la IA.
- Art. 11: que garantiza la protección en los tratamientos de datos personales que se realicen en el entorno controlado de pruebas.
- Art. 31: que permite la utilización de datos personales legalmente recopilados con otros fines para el entrenamiento y validación de sistemas de IA innovadores, respetando lo dispuesto en el RIA y el RGPD.
- Art. 33: que permite obtener datos para el entrenamiento y validación de los sistemas de IA utilizando técnicas de raspado de datos desde sitios web, portales públicos, perfiles, revistas, o documentos.
- Art. 35: que se remite para la protección de datos personales durante el ciclo de vida de los sistemas de IA a lo previsto, entre otras normas, en el RGPD, la LOPDP, y el RIA.

Para concluir este apartado diremos que la mayoría de las Comunidades Autónomas (CCAA) han intentado potenciar buenas prácticas en este campo como pueden ser los cursos de formación, en especial para el profesorado, con el fin de promover el uso pedagógico, legal y ético de la IA en el ámbito educativo.

3. Aplicaciones de la inteligencia artificial en el ámbito educativo

Antes de comenzar este apartado, y aunque pueda resultar obvio, es preciso hacer una aclaración.

Las aplicaciones de la IA en el ámbito educativo a las que vamos a hacer referencia son aquellas que se van a utilizar de modo sistemático, organizado y planificado tanto para la formación y evaluación del alumnado en el marco de los centros docentes, como por parte de las Administraciones educativas para la gestión de los aspectos administrativos necesarios para la prestación de dicho servicio.

Estos usos, como ya se advirtió con anterioridad, son propuestos, planificados, dirigidos y controlados por las Administraciones, que a su vez pueden tener potestad para negociar sus condiciones con los prestadores del sistema de IA.

Quedan excluidos pues de este epígrafe los usos que, a título particular, puedan hacer tanto el alumnado y sus familias como el profesorado, aunque estos usos puedan presentar estrecha relación con la realización o preparación de tareas escolares, pues este uso no puede ser dirigido ni controlado, ni queda sometido a condiciones negociadas, sino a meros contratos de adhesión[25] en los que el particular no goza de potestad alguna para proponer, imponer o rechazar condición alguna distinta de las expresamente fijadas por la parte proponente; sólo puede pues, aceptar pura y simplemente o no contratar.

Hecha esta salvedad, es preciso partir de la base de que, si es la Administración educativa la que impone el uso de uno o varios sistemas de IA para su funcionamiento, tanto administrativo, como educativo, es dicha Administración la que debe velar por el respeto de la normativa vigente tanto en materia de IA como de protección de datos, del alumnado, de sus familias, del profesorado o del personal de los centros.

Pero, aunque no sea objeto de este estudio, pues como se ha advertido no se aborda la utilización de sistemas de IA a título particular, no estará de más recordar a partir de qué edad es posible consentir en el ámbito europeo en general, y en España en particular, la cesión y tratamiento de datos personales.

Como novedad del RGPD, desde mayo de 2018 no pueden ofrecerse servicios de la sociedad de la información a menores de 16 años sin el consentimiento paterno

[25] Contratos de adhesión o contratos tipo son aquellos cuyas cláusulas son redactadas por una sola de las partes, sin intervención de la otra, quedando con ello limitada la voluntad de esta última a aceptar pura y simplemente las estipulaciones establecidas, es decir adherirse al contrato, o a no suscribir el contrato.

o materno, o del tutor legal, salvo que una ley nacional establezca una edad inferior que, en ningún caso, será inferior a 13 años.

No obstante, en España, la LOPDP 2018 establece, salvo excepciones legales, la posibilidad de recabar datos personales de mayores de 14 años sin necesidad de obtener el consentimiento de sus progenitores (art. 7.1 LOPDP 2018)[26].

3.1 Utilización de la IA para la preparación de clases, materiales, recursos y tareas académicas

Probablemente este sea uno de los usos más actuales y frecuentes por parte del profesorado, y también de los que implican, en general, menor riesgo para el objeto principal de este estudio, es decir para protección de datos.

En principio, encomendar a un sistema de IA la tarea de buscar materiales didácticos, preparar presentaciones o crear actividades formativas no debe suponer peligro alguno para el alumnado, desde el punto de vista de la privacidad.

Esto no implica, que no haya otros riesgos potenciales que exijan una labor de verificación o comprobación por parte de los responsables docentes, ya que no existe una garantía absoluta sobre la integridad, veracidad[27] o la ausencia de sesgos[28] discriminatorios en los datos, informaciones o materiales facilitados por la IA.

Lo que puede constituir un serio riesgo para el proceso de aprendizaje del alumnado es el uso sistemático y no dirigido por parte del mismo para la resolución de estas tareas. Tal y como advierte González de la Garza (2024, p. 128), “estas tecnologías son inhibidoras de la implicación personal en el descubrimiento autónomo del saber que es esencial en el aprendizaje”.

Sin embargo, y como ya se advirtió con anterioridad, este último tipo de uso, salvo encomienda específica por parte del profesorado y tutelada en el aula como

[26] Sin embargo, el proyecto de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales, si finalmente entra en vigor, pretende elevar esta edad hasta los 16 años en nuestro país.
[27] Es lo que se ha venido a denominar como “alucinaciones” de la IA, es decir, resultados engañosos, irreales o incorrectos, derivados de un entrenamiento de la IA con datos inexactos o insuficientes, de la realización de suposiciones incorrectas, o de errores sistemáticos derivados del hecho de favorecer una información en detrimento de otras (sesgo). Véanse M. Fuertes López (2024, pp. 155 y 156) y Mª. J. Jiménez Linares (2024, p. 274).
[28] Sobre los posibles sesgos en la información facilitada por los sistemas de IA y sus efectos puede verse L. M. González de la Garza (2024, pp. 132 a 137).

actividad formativa, entra exclusivamente dentro del ámbito privado no susceptible de control por las Administraciones educativas.

3.2 Plataformas de aprendizaje adaptativo

Uno de los mayores retos planteados en el ámbito educativo en la actualidad es la atención a la diversidad del alumnado y la personalización del aprendizaje[29].

El análisis masivo de datos sobre trabajo y rendimiento del alumnado permite prever situaciones de dificultad de aprendizaje y, con ello, diseñar estrategias para solventar las dificultades anticipadas o previstas, o incluso, simplemente, mejorar el rendimiento ya satisfactorio, a través de fórmulas de aprendizaje más eficiente.

Ahora bien, estas técnicas de trabajo requieren del análisis de información personalizada de cada alumno/a y de datos relativos a capacidades, intereses, motivaciones, estrategias y dificultades de aprendizaje.

La IA ofrece incluso la posibilidad de adaptar el aprendizaje del alumnado con necesidades especiales o con discapacidad, pero para dicha adaptación se hace necesario dejar constancia de estas circunstancias, lo que ya supone conocimiento de datos personales especialmente sensibles.

En este sentido es preciso recordar que, tal y como ya se dijo con anterioridad al hacer referencia a la legislación vigente, el RIA, en su Considerando 56 y en el anexo III incluye dentro de la categoría de sistemas de IA de alto riesgo aquellos que puedan ser “utilizados para evaluar los resultados del aprendizaje, también cuando dichos resultados se utilicen para orientar el proceso de aprendizaje de las personas físicas en centros educativos y de formación profesional a todos los niveles” y los “utilizados para evaluar el nivel de educación adecuado que recibirá una persona o al que podrá acceder, en el contexto de los centros educativos y de formación profesional o dentro de estos a todos los niveles”.

Los requisitos que deben cumplir los sistemas de IA de alto riesgo se regulan en la sección 2 del capítulo III del RIA (arts. 8 a 15), y hacen referencia al establecimiento de un sistema de gestión de riesgos; la calidad y gobernanza de los datos de entrenamiento, validación y ensayo; elaboración de la documentación técnica

[29] Sobre el particular puede verse C. Paredes Gallardo (2024, pp. 518 y ss.).

necesaria; mantenimiento de registros de eventos durante su vida útil; transparencia y suministro de información para el uso de la IA a las empresas; posibilidad de supervisión humana; y necesidad de alcanzar un grado suficiente o un nivel adecuado de precisión, solidez o robustez, y ciberseguridad.

A esto debe añadirse, la obligación de cumplir con la normativa del RGPD, y de la LOPDP en nuestro país, si la adaptación del aprendizaje a través de sistemas de IA exige o requiere el uso de datos personales de identificación del alumnado usuario, o de otros especialmente sensibles como los relativos al origen racial o salud de los usuarios (art. 9 nos 1 y 2 del RGPD)[30].

El consentimiento para el tratamiento de datos personales se rige por las condiciones establecidas en los arts. 7 y 8 del RGPD, artículos que deben ser interpretados de conformidad con lo dispuesto en el Considerando 32 de dicha norma.

En nuestro país, la LOPDP de 2018 establece, salvo excepciones legales, la posibilidad de recabar datos personales de mayores de 14 años, sin necesidad de obtener el consentimiento de sus progenitores (art. 7.1 de la LOPDP), si bien esta edad puede ampliarse hasta los 16, si se aprueba en el futuro el proyecto de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales.

3.3. Sistemas de evaluación automatizada del aprendizaje y sistemas de *proctoring*[31].

Tal y como ya se dijo anteriormente, el anexo III del RIA en su número 3 considera sistemas de alto riesgo en el campo de la educación y formación profesional,

> b) Los sistemas de IA destinados a ser utilizados para evaluar los resultados del aprendizaje, también cuando dichos resultados se utilicen para orientar el proceso de aprendizaje de las personas físicas en centros educativos y de formación profesional a todos los niveles.

[30] El art. 9.1 del RGPD establece una prohibición estricta de tratamiento de datos personales relativos al origen étnico o racial, así como también de datos relativos a la salud, vida y orientación sexual, salvo en aquellos supuestos en los que pueda concurrir alguna excepción de las previstas en su nº 2, entre las que cabe destacar, a los efectos que nos interesan para este estudio, el consentimiento explícito de la persona interesada y con fines específicos.

[31] El *proctoring* es un sistema de supervisión remota de exámenes que utiliza tecnología como cámaras web, inteligencia artificial y software para garantizar la integridad y veracidad de las evaluaciones online, previniendo el fraude, el plagio o la suplantación de identidad.

c) Sistemas de IA destinados a ser utilizados para evaluar el nivel de educación adecuado que recibirá una persona o al que podrá acceder, en el contexto de los centros educativos y de formación profesional o dentro de estos a todos los niveles.

d) Sistemas de IA destinados a ser utilizados para el seguimiento y la detección de comportamientos prohibidos por parte de los estudiantes durante los exámenes en el contexto de los centros educativos y de formación profesional o dentro de estos a todos los niveles.

Así pues, deben cumplirse también en este caso los requisitos de los arts. 8 a 15 del RIA y los relativos a protección de datos del RGPD y de la LOPDP.

Además, de acuerdo con lo previsto en el Considerando 73 del RIA "los sistemas de IA de alto riesgo deben diseñarse y desarrollarse de tal modo que las personas físicas puedan supervisar su funcionamiento, así como asegurarse de que se usan según lo previsto (…)".

Esta obligación queda plasmada en el art. 14 de la citada norma que se expresa en los siguientes términos:

Supervisión humana

1. Los sistemas de IA de alto riesgo se diseñarán y desarrollarán de modo que puedan ser vigilados de manera efectiva por personas físicas durante el período que estén en uso, lo que incluye dotarlos de herramientas de interfaz humano-máquina adecuadas.
2. El objetivo de la supervisión humana será prevenir o reducir al mínimo los riesgos para la salud, la seguridad o los derechos fundamentales que pueden surgir cuando se utiliza un sistema de IA de alto riesgo conforme a su finalidad prevista o cuando se le da un uso indebido razonablemente previsible (…).

Esto significa pues, que cualquier sistema de evaluación automatizada del aprendizaje del alumnado ha de ser siempre supervisado por el profesorado responsable y competente, profesorado que ha de estar adecuadamente formado para "entender adecuadamente las capacidades y limitaciones pertinentes del sistema de IA de alto riesgo y poder vigilar debidamente su funcionamiento (…)" (arts. 14.4 y 26.2 RIA).

Para concluir este apartado, unas breves consideraciones en relación con los sistemas de vigilancia remota de exámenes o *proctoring*, que ciertamente no suelen ser habituales en enseñanza primaria, secundaria, bachillerato o FP, salvo en modalidades de formación a distancia, o situaciones extremas como la pandemia por COVID-19[32].

Al margen de la resistencia de alumnado y profesorado hacia esta modalidad de vigilancia, por la percepción negativa que se tiene de dichos sistemas, y la posible invasión de la privacidad, cierto es también que puede verse seriamente afectada por problemas técnicos como deficiencias de conexión a internet de los propios centros docentes o de los estudiantes, incompatibilidad de dispositivos o programas, etc.

Dejando al margen dichos problemas técnicos, y partiendo de la hipótesis de inexistencia de brecha digital de los usuarios, aún podemos hacer referencia a otras dificultades.

Los sistemas de *proctoring* se basan en tecnologías que combinan el reconocimiento facial, la biometría[33] y sistemas de inteligencia artificial.

Así pues, estos sistemas utilizan datos personales para el cumplimiento de su función y, por ello, quedan sujetos al cumplimiento de la normativa sobre protección de datos personales vigente en nuestro país y en el ámbito europeo.

La IA, por su parte, cumple además la misión de identificar actuaciones o actividades sospechosas durante la realización de un examen, que pueden requerir revisión humana.

El *proctoring*, además de la propia identificación del estudiante mediante datos biométricos, puede ampliarse al control del entorno de la persona examinada (ej.

[32] Sobre el uso de técnicas de reconocimiento facial en la realización de pruebas de evaluación online a raíz de la pandemia por COVID-19 puede verse el informe de la AEPD 0036/2020, de mayo de 2020, accesible en la web https://www.aepd.es/documento/2020-0036.pdf

[33] Sobre datos biométricos véase el considerando 54 del RIA. El art. 4.14 del RGPD define los datos biométricos como “aquellos 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”. Así pues, estos datos biométricos son datos personales, que permiten la identificación de cualquier persona, y que, por tanto, quedan sujetos al estricto cumplimiento de la normativa ya conocida, en especial del RGPD y de la LOPDP. Sobre el particular puede verse asimismo la “Guía sobre tratamientos de control de presencia mediante sistemas biométricos” de la Agencia Española de protección de Datos (AEPD), publicada en noviembre de 2023. Véase noticia de su publicación y link de acceso en https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/la-aepd-publica-una-guia-sobre-la-utilizacion-de-datos

presencia de otros sujetos, materiales, libros, fuentes de información, transmisiones de audio, recursos tecnológicos de apoyo, etc.).

Entre los riesgos derivados de este tipo de supervisión tecnológica podemos citar una posible invasión de la privacidad derivada del control del entorno de la persona examinada, en especial si es un domicilio[34], y también la posibilidad de que se produzcan comportamientos inocentes detectados como falsos positivos de conductas irregulares.

En nuestro país, este asunto también ha suscitado polémica en algunos supuestos, inicialmente derivados de la necesidad de realizar exámenes a distancia durante la pandemia por COVID-19[35], pero que se han extendido con posterioridad a otro tipo de situaciones académicas en las que la fórmula del *proctoring* no quedaba amparada por circunstancias tan excepcionales, y en las que la AEPD ha dictado resoluciones más restrictivas y de aplicación más estricta de la normativa de protección de datos, por ejemplo en aquellos casos en los que se ha pretendido utilizar esta modalidad de examen y vigilancia remota, pero sin ofrecer garantías suficientes o métodos alternativos menos invasivos de la privacidad, si bien la misma EAPD ha apuntado futuras posibilidades normativas para justificar su admisibilidad[36].

[34] Sobre esa posible invasión de la privacidad véase el caso Ogletree contra la Universidad Estatal de Cleveland, n.° 1:2021cv00500 - Documento 37 (ND Ohio 2022). El caso "Ogletree vs. Cleveland State University" hace referencia a una demanda presentada por el estudiante Aaron Ogletree contra la Universidad Estatal de Cleveland por violar su derecho a la privacidad, alegando que el requisito de realizar un escaneo de su habitación antes de un examen remoto era un registro irrazonable y una violación de la Cuarta Enmienda de la Constitución americana. El tribunal falló inicialmente a favor de Ogletree, pero la decisión fue anulada posteriormente por razones procesales. En nuestro país este asunto también ha suscitado polémica en algunos supuestos, fundamentalmente derivados de la necesidad de realizar exámenes a distancia durante la pandemia por COVID-19.

[35] Sobre el particular puede verse el Expediente nº EXP202200367 (AI/00086/2022, de 21 de octubre de 2022) de la AEPD derivado de las reclamaciones remitidas por la Asociación de estudiantes UNIR y otros contra la UNIR, por el tratamiento de datos derivado de los sistemas reconocimiento y vigilancia para la realización de exámenes a distancia, sistema que obligaba a instalar en los ordenadores personales una herramienta específica que permitía el uso de la cámara web frontal para registrar la imagen del estudiante mientras realiza su examen, y también la captura de acciones realizadas en el escritorio, con el teclado y el ratón, a lo que se unía además como requisito obligatorio la instalación de una segunda cámara, además de la frontal que ya se venía utilizando, obligando a que dicha cámara enfoque el entorno del alumno, y se visualicen sus dos manos, su cuerpo y sus pantallas de trabajo, de forma que se vea claramente lo que está haciendo. De no hacerlo así, y según se denuncia, el estudiante obtendrá la calificación de cero en el examen, pudiendo motivar la pérdida de la evaluación continua. Considera en este supuesto la AEPD que no puede acreditarse el tratamiento de datos biométricos, por lo que procede al archivo del caso.

[36] Véase noticia publicada por la AEPD en su página web con fecha de 3 de junio de 2025, que incluye la fundamentación jurídica de la resolución correspondiente: https://www.aepd.es/informes-y-resoluciones/criterios-juridicos-aepd/aepd-sanciona-tratamiento-datos-biometricos-ia (resolución no publicada a fecha de entrega de esta artículo).

3.4 *Chatbots* y tutores virtuales

Podemos definir o explicar el *chatbot* como un programa informático con IA, que imita o simula conversaciones de texto, o incluso de voz, como si se estuvieran manteniendo con un ser humano, logrando con ello una interacción que permite responder preguntas o proporcionar información, sin intervención humana, y por tiempo ilimitado.

Dadas sus amplias prestaciones, la posibilidad de uso en el ámbito educativo es considerable, ya que permite resolver dudas en tiempo real, crea nuevas formas de participación y colaboración, e incluso puede ser un recurso de apoyo al aprendizaje.

No obstante, como todos los supuestos analizados con anterioridad, no está exento de riesgos, entre los cuales cabe citar, si no se adoptan las medidas de seguridad adecuadas, el acceso no autorizado a datos personales[37] (especialmente grave en el caso de alumnado menor de edad), respuestas erróneas o sesgadas en relación con las preguntas planteadas, o incluso suplantaciones de personalidad.

Así pues, cualquier chatbot utilizado en el ámbito educativo debe contar con medidas de seguridad reforzadas y adaptadas al cumplimiento del RGPD y la LOPDP.

Y para cerciorarnos de que un *chatbot* cumple con la normativa del RGPD, debemos verificar que nos ofrece un aviso de privacidad, que se identifica con claridad al responsable del tratamiento de datos, y que permite el ejercicio y salvaguarda de nuestros derechos.

Precisamente por ello la AEPD hace las siguientes recomendaciones para el uso de un chatbot: extremar la precaución a la hora de facilitar información o datos personales; no facilitar datos superfluos o innecesarios para la utilización del *chatbot*; no dar consentimientos genéricos en los que no se especifique el uso de los datos o sin posibilidad de revocación de dicho consentimiento; no facilitar datos cuando pueda producirse una trasferencia internacional de los mismos a países no obligados por la normativa del RGPD, o que no ofrecen garantías suficientes de protección.

[37] Entre los datos personales que puede recopilar un *chatbot* cabe destacar el nombre de usuario, la dirección de correo electrónico, IP, hábitos o costumbres de uso, así como cualquier otro que se pueda utilizar o transmitir en la conversación, incluidos pensamientos, sentimientos, opiniones o ideas.

Por su parte, las herramientas de tutoría virtual o inteligente se basan en el análisis de los mecanismos de aprendizaje del alumnado, lo cual permite una adaptación de los contenidos educativos y ofrece un aprendizaje más personalizado.

Los riesgos propios de la utilización de este tipo de tecnologías no difieren en sustancia de los estudiados con anterioridad, sobre todo, los derivados de una integración apresurada en los centros docentes que pueda provocar serios perjuicios en relación con la privacidad, la equidad y la fiabilidad de las informaciones obtenidas.

3.5 Análisis predictivo y *big data* educativo

Gracias al análisis masivo de conjuntos de datos muy variados y procesados en un escaso margen de tiempo (*big data*) es posible extraer información de gran interés para predecir y prevenir situaciones futuras como el riesgo de fracaso escolar o de absentismo, entre otras.

La gran cantidad de información acumulada y analizada permite una intervención temprana, anterior a situaciones de fracaso escolar, la personalización del aprendizaje, una retroalimentación adecuada de las tareas etc. El análisis predictivo aporta información y facilita la toma de decisiones, pero no debe sustituir el criterio humano adoptado por profesionales de la educación.

La utilización de este tipo de tecnologías requiere de una infraestructura tecnológica adecuada, una buena preparación del profesorado, la utilización de datos y algoritmos apropiados, y el cumplimiento de la normativa vigente en materia de IA y de protección de datos.

Entre los riesgos derivados de su utilización nos encontramos con los posibles sesgos contenidos en los datos con los que ha sido entrenada la IA, diagnósticos equivocados de situaciones de riesgo obtenidos a partir de datos estadísticos y de probabilidades que no crean necesariamente certezas, o la probable estigmatización asociada a las etiquetas asignadas por estas técnicas analíticas.

Para prevenir estos riesgos la AEPD editó ya en 2017 el denominado “Código de buenas prácticas en protección de datos para proyectos Big Data”[38]

Dicho código propone medidas en relación con la protección de datos como la transparencia de la información facilitada a los usuarios respecto al tratamiento de sus datos; la necesidad de recabar el consentimiento expreso y explícito para la gestión de dichos datos, con conocimiento expreso de su finalidad; la anonimización de los datos; el uso de estrategias reforzadas de seguridad como el cifrado de datos; que las entidades que deseen desarrollar proyectos de *Big data* acaten de manera expresa el cumplimiento del RGPD; o la evaluación de impacto de la protección de datos (EIPD) tanto por parte de las empresas o compañías como de las Administraciones públicas, en este caso educativas.

3.6 Tareas de gestión administrativa de los centros docentes y de las Administraciones públicas

Aunque inicialmente podamos pensar que las tareas burocráticas y administrativas puedan ser el paradigma de actuaciones normalmente estructuradas y repetitivas, y por ello susceptibles de ser encomendadas a una IA, debemos tomar esta afirmación con suma cautela, especialmente en el ámbito educativo.

Dentro de las tareas de gestión administrativa propias de un centro docente y de las Administraciones educativas[39] podemos citar, entre otras, los controles de asistencia del alumnado o del profesorado, la gestión de la documentación académica (ej. solicitud de admisión, documento de matriculación, solicitud de títulos académicos, convalidaciones…), informes, memorias, comunicaciones administrativas, solicitudes de becas etc.

Una buena parte de esta documentación administrativa contiene o incluye datos personales relevantes o especialmente sensibles.

Cualesquiera documentos administrativos de solicitud a las Administraciones educativas, o de incorporación a un centro docente, llevan los datos de identificación

[38] Dicho código puede encontrase en la web www.aepd.es/documento/guia-codigo-de-buenas-practicas-proyectos-de-big-data.pdf junto con un conjunto muy numeroso de herramientas, documentos, instrucciones, informes, modelos etc., publicados por la AEPD, en la web https://www.aepd.es/areas-de-actuacion/innovacion-y-tecnologia

[39] Véase noticia publicada en el Periódico de Aragón con fecha de 20 de abril de 2025, en la que se afirma que “El Gobierno de Aragón estudia aplicar la IA para el proceso de matriculación escolar”. Noticia recuperada a partir de https://www.elperiodicodearagon.com/aragon/2025/04/20/gobierno-aragon-estudia-aplicar-ia-116524587.html .

completos del alumnado, y muy probablemente también, los de sus familiares más cercanos.

Los impresos de matrícula o de solicitud de admisión pueden contener datos relativos a la elección de asignaturas o materias que impliquen manifestación de opciones relativas a creencias religiosas, a situaciones de discapacidad, hacer referencia al origen racial o étnico, especificar situaciones familiares (separación, divorcio, familias monoparentales, víctimas de violencia de género…).

Los informes de los departamentos o equipos de orientación pueden hacer referencia asimismo a varias de las situaciones anteriormente citadas, y también a trastornos personales del aprendizaje (ej. TDAH), necesidad de adaptaciones curriculares, etc.

Las solicitudes de becas y ayudas al estudio contienen además datos relevantes y confidenciales sobre la situación económica personal y familiar.

Los controles de asistencia del alumnado o del profesorado suelen incorporar documentación justificativa de ausencias por causas médicas, motivos personales o familiares que pueden afectar a la privacidad.

El listado de citas de este tipo sería prácticamente interminable, y no debemos olvidar que, además de afectar a menores de edad en muchos casos, nos podemos encontrar dentro de los supuestos ya explicados con anterioridad de uso de sistemas de IA de alto riesgo del anexo III del RIA, en conexión con el art. 6 apdo. 2 de la misma norma, en particular, “para determinar el acceso o la admisión de personas físicas a centros educativos y de formación profesional a todos los niveles o para distribuir a las personas físicas entre dichos centros” (apdo. 3.a); ante sistemas de IA “utilizados para evaluar los resultados del aprendizaje, también cuando dichos resultados se utilicen para orientar el proceso de aprendizaje” (apdo. 3.b); o los “destinados a ser utilizados para evaluar el nivel de educación adecuado que recibirá una persona o al que podrá acceder, en el contexto de los centros educativos y de formación profesional o dentro de estos a todos los niveles” (apdo. 3.c).

Así pues, si nos encontramos ante supuestos de sistemas de IA de alto riesgo la observancia y el cumplimiento de la normativa vigente, en especial del RIA, del RGPD[40] y la LOPDP ha de ser estricta[41].

Mención destacada pueden merecer también en este campo de las tareas de gestión administrativa de las Administraciones públicas, aquellas aplicaciones prácticas del uso de la IA que se pueden hacer desde la Inspección de Educación[42].

Entre ellas cabría destacar la sistematización de tareas documentales (ej. realización de informes repetitivos, redacción de actas, resumen y análisis de documentos extensos o complejos y de normativa etc.); la predicción del fracaso escolar, con el fin de asesorar a los centros de forma anticipada; o la búsqueda y análisis de normativa vigente etc.

A su vez, esa extraordinaria capacidad de la IA para el estudio y examen de grandes cantidades de datos (*big data*), puede facilitar los procesos de toma de decisiones, de realización de estudios, de planes de mejora, de análisis de políticas educativas etc.

Todo ello va a requerir de un adecuado proceso formativo de la Inspección y de adaptación a la educación del siglo XXI, incluso una posible especialización[43].

3.7 Sustitución de los libros de texto por dispositivos digitales

Tal vez sea esta una de las cuestiones que está suscitando mayor polémica en la actualidad[44], por el amplio debate abierto en relación con los beneficios y riesgos derivados de la utilización de dispositivos digitales en sustitución de los tradicionales libros de texto y todo lo que ello implica, no sólo en relación con la metodología docente, sino también con la protección de los menores.

[40] El RGPD también incluye los conceptos de riesgo y alto riesgo en relación con la protección de datos personales, Así el art. 32 hace referencia a la necesidad de tener en cuenta los riesgos por parte de los responsables del tratamiento, y el art. 35 exige a dichos responsables, en los casos de alto riesgo, la realización de una evaluación de impacto relativa a la protección de datos.
[41] *Vid*. supra los apartados dedicados al RIA, al RGPD y a la LOPDP y a las obligaciones de protección de los usuarios impuestas por los mismos.
[42] Véanse sobre el particular J. F. Álvarez Aguilar y M. T. Acisclos García (2025).
[43] Véase al respecto F. Tébar Cuesta (2020).
[44] Véase el artículo que lleva por título “¡Stop pantallas!” publicado en el suplemento de prensa XL Semanal nº 1981, de 12 de octubre de 2025 y en xlsemanal.com.

Dejando al margen los aspectos puramente metodológicos y centrándonos en los riesgos relativos a la protección de datos, es preciso recordar que cada vez más centros docentes, incluso de educación infantil y primaria, se sirven de dispositivos y herramientas digitales[45] para sus procesos de enseñanza y aprendizaje, siguiendo un sistema de sustitución de los libros de texto tradicionales que, prácticamente, no deja otra posible alternativa a los estudiantes y sus familias.

Aunque el objetivo de aumentar las competencias digitales del alumnado pueda ser muy loable, lo cierto es que el modelo pedagógico del "*one to one*" (un alumno/un ordenador) entraña riesgos evidentes para la seguridad de los menores.

Y así se puso de manifiesto en un informe emitido por el Gabinete Jurídico de la AEPD en 2024[46] en el que se informaba desfavorablemente la firma del Convenio de uso en los centros docentes, de *Google Workspace for Education*.

En dicho informe se consideraba que el Acuerdo-Convenio que el INTEF iba a suscribir con Google Cloud EMEA Limited, para que se implementara en las aulas educativas competencia del Ministerio de Educación y FP el uso de la "Solución tecnológica Workspace for Education", vulneraba la normativa vigente, y, en concreto, el RGPD y la LOPDP.

Dicha vulneración, de modo muy resumido, se basaba en un acopio excesivo e invasivo de información personal, en la posibilidad de usar dicha información para elaborar perfiles, y en el riesgo de que toda esta información pueda ser transferida, bajo el amparo de un presunto interés legítimo, a terceros países no sujetos a las reglas de protección del RGPD.

4. Principales riesgos y desafíos del uso de la IA y protección de datos

Aunque se ha hecho referencia en los apartados anteriores a una buena parte de los riesgos derivados del uso de sistemas de IA en relación con la protección de datos,

[45] Hoy en día no es extraño el uso en buena parte de los centros docentes, públicos o privados de *tablets*, dispositivos Chromebook etc., que se sirven de herramientas digitales de empresas como Apple; Microsoft y Google, herramientas que acumulan gran cantidad de datos tanto personales como de navegación y comportamiento de los usuarios.

[46] Informe 0050/2023, publicado en febrero de 2024. Véase en la web https://www.aepd.es/documento/2023-0050.pdf

conviene recordar y sistematizar brevemente los más relevantes dada la trascendencia y gravedad que pueden tener en el ámbito educativo.

4.1 Datos de menores

En primer lugar, es preciso tomar en consideración que una buena parte de los datos personales del sector educativo, hacen referencia a menores de edad.

Además, de acuerdo con la legislación vigente (art. 7.1 LOPDP), y a salvo de modificaciones que se pretende introducir y están pendientes de tramitación parlamentaria[47], los menores de edad, pero mayores de 14 años pueden prestar su consentimiento en nuestro país, sin que sea necesaria la concurrencia de sus progenitores.

No es difícil pensar en la facilidad con la que un menor de esa edad puede otorgar su consentimiento a cambio de una hipotética "recompensa inmediata" (ej. posibilidad de probar un juego en modo demostración, descargar programas de forma gratuita etc.) ofrecida por el propietario/a de una página web o por un sistema de IA, interesado en captar información relativa a sus datos personales.

Si hacemos referencia a algunos de los riesgos intrínsecos y de mayor gravedad derivados del uso de datos de menores, podemos incluir según la AEPD[48] los siguientes: el uso fraudulento y sin autorización de imágenes, incluso manipuladas; la geolocalización de los menores (supuesto especialmente grave en casos de violencia de género o intrafamiliar); la falta de privacidad, el ciberacoso, el *grooming* (ciberacoso sexual); o incluso pedofilia.

4.2 Decisiones automatizadas y perfilado de datos

De conformidad con lo dispuesto en el art. 22 del RGPD podemos considerar decisiones individuales automatizadas aquellas que, concerniendo a un interesado, se basan únicamente en el "tratamiento automatizado de datos personales, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar". Es decir, que el tratamiento automatizado de

[47] Véase el Proyecto 121/000052 de Ley Orgánica para la protección de las personas menores de edad en los entornos digitales, publicado en el Boletín Oficial de las Cortes Generales (Congreso de los Diputados), de 11 de abril de 2025, en especial su disposición final sexta que amplía hasta a los 16 años la edad mínima para prestar el consentimiento.
[48] Véase https://www.aepd.es/prensa-y-comunicacion/blog/los-riesgos-del-sharenting-en-la-vida-de-los-menores

datos en este caso supone la ausencia de participación humana en el proceso de decisión[49].

¿En qué supuestos podría afectar pues este tipo de decisiones automatizadas y perfilado de datos, o suponer un riesgo para la educación? Pues podría afectar gravemente a los procesos de acceso o selección de personas a la educación, o a centros docentes concretos a los que se ha formulado una solicitud de ingreso, incluidos lógicamente los universitarios.

4.3 Transferencias internacionales de datos

Las transferencias internacionales de datos se producen cuando se da una circulación o movimiento de datos con origen en territorio español, y destino en países que se encuentran fuera del Espacio Económico Europeo (EEE), es decir, la zona en la que se hallan todos los países de la Unión Europea (UE) y Liechtenstein, Islandia y Noruega.

Es posible, desde el punto de vista legal, que los responsables y encargados del tratamiento de datos realicen dichas transferencias internacionales de datos sin la concurrencia de la pertinente autorización de la AEPD, en el caso de que se observen las reglas establecidas en el RGPD.

Cabe asimismo la posibilidad de que se produzca igualmente una transferencia internacional de datos en otros supuestos excepcionales[50].

¿Cuáles son pues los riesgos derivados de las transferencias internacionales de datos? Rara vez somos conscientes del lugar en el que se alojan nuestros datos cuando prestamos un consentimiento, sobre todo si es apresurado. Desconocemos pues las consecuencias que de ello puedan derivar para la utilización de nuestros datos, según la normativa aplicable en el lugar en el que radican.[51]

---

[49] Véanse las Directrices WP 251 sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679.

[50] Para más información véase https://www.aepd.es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/garantias-transferencias-datos-personales

[51] En concreto, los datos recabados por ChatGPT se alojan en los servidores de OpenAI. Según manifiesta OpenAI con fecha de 8 de mayo de 2025, “para los clientes de la API (Plataforma para la creación de aplicaciones de IA) que cumplan los requisitos y para los nuevos espacios de trabajo ChatGPT Enterprise y Edu, la residencia de datos en reposo no solo se ha ampliado a Europa, sino también a Estados Unidos, Japón, Canadá, Corea del Sur, Singapur e India”. Véase https://openai.com/es-419/index/introducing-data-residency-in-europe/ En el caso de Gemini, se pone de manifiesto que se trata de una empresa mundial y, por consiguiente, “la Información personal puede almacenarse y procesarse en cualquier país donde tengamos operaciones, afiliadas, socios externos o

El almacenamiento de datos en la nube es un negocio emergente, ofrecido por muchas empresas. Presenta como ventajas principales poder disponer de los datos en cualquier lugar, y que, en caso de avería o siniestro, no se pierdan los datos grabados.

Su inconveniente principal, como ya se ha advertido, reside en el hecho de que se desconoce dónde radican físicamente esos datos, por lo que incluso se pueden encontrar en terceros países que no garanticen legalmente el mismo nivel de protección que España, la UE o el EEE.

No obstante, en los casos de uso de los sistemas de IA en el ámbito docente, deberían ser los responsables del tratamiento (Administraciones educativas para los centros públicos y entidades titulares para los privados y concertados), quienes garantizasen la protección de los datos necesarios en el proceso de enseñanza y aprendizaje, en toda su extensión.

4.4 Sesgos algorítmicos y discriminación

Aunque, con anterioridad, se ha hecho ya referencia reiterada a los sesgos derivados del uso de sistemas de IA, y sus posibles consecuencias discriminatorias, es preciso recordar de nuevo que la cuestión queda ampliamente regulada por el RIA, en especial, en su art. 10.2, letras f y g.

Los sesgos discriminatorios derivan de resultados obtenidos por un sistema de IA en cuyo origen, entrenamiento, aprendizaje, información acumulada o algoritmo utilizado, se han alojado, incluso de forma no intencionada, suposiciones erróneas, prejuicios sistemáticos, informaciones falsas, etc.

Estos sesgos pueden tener una amplia repercusión en el ámbito educativo en aquellos casos en los que se utilice un sistema de IA, por ejemplo, para evaluar el rendimiento del alumnado, para personalizar la enseñanza o para la toma de decisiones, sobre todo si estas están automatizadas, y se desarrollan sin intervención humana.

---

donde contratemos proveedores de servicios. Gemini, sus afiliadas, socios externos o proveedores de servicios pueden transferir, almacenar y procesar tu Información personal en todo el mundo, incluso en Irlanda, el Reino Unido, Malta, Singapur y los EE. UU.” Véase https://www.gemini.com/es-LA/legal/privacy-policy . Ambas empresas afirman cumplir con lo dispuesto en el RGPD en el contexto europeo, pero siguen planteándose quejas y reclamaciones al respecto.

Así podemos llegar a consecuencias indeseadas como desviar recursos de quienes verdaderamente los necesitan, mantener desigualdades o discriminaciones existentes con anterioridad, y con ello afectar a decisiones fundamentales como las relativas a la asignación de recursos educativos, admisión a programas, etc., privilegiando de esta manera, o perjudicando en su caso, a ciertos grupos de estudiantes por razón de su origen racial o condición social o demográfica. Aplicando estos criterios discriminatorios vulneramos el principio de igualdad de oportunidades, reforzamos estereotipos y mantenemos la brecha educativa.

4.5 Seguridad y brechas de datos

El *hackeo* o pirateo informático supone, como bien sabemos, un ataque o entrada no autorizados en el contenido de un dispositivo, red o sistema informático, aprovechándose de la fragilidad de sus medios o sistemas de seguridad, para sustraer información o datos, con el fin de causar un daño o cometer cualquier tipo de fraude (por ej. actividades delictivas como robos de identidad o dinero, comercio ilegal de datos etc.).

Aunque quizás pueda pensarse que el sector educativo no es excesivamente interesante para el *hackeo* a gran escala de datos, por la escasa trascendencia de estos en comparación con otros sectores (ej. banca y comercio electrónico, sistemas e instalaciones militares, grandes empresas, sector sanitario, Administraciones públicas etc.), lo cierto es que, quizás por su fácil vulnerabilidad, es uno de los más afectados[52].

Esta vulnerabilidad o exposición al *hackeo* deriva en gran medida del alto grado de digitalización del sector docente (plataformas educativas como Moodle, o Classroom, pizarras digitales, trabajo en la nube, etc.), de la interconexión existente

[52] Aunque las noticias en este sentido son constantes, véase, por ejemplo, la noticia publicada por El Periódico de Aragón con fecha de 23 de julio de 2025 y en la que se advertía que el propio Departamento de Educación del Gobierno de Aragón había reconocido que la aplicación SIGPEAC (Sistema Integrado de Gestión del Procedimiento de Evaluación y Acreditación de Competencias) había sufrido un *hackeo* con fecha de 16 de julio, a raíz del cual un "pirata informático logró acceder a datos -en concreto al nombre y correo electrónico- de algunos profesores que son usuarios en la misma." (Acceso en la web https://www.elperiodicodearagon.com/aragon/2025/07/23/hackean-aplicacion-educacion-datos-profesores-119988347.html) Asimismo, la Consejería de Educación de Castilla y León informó que con fecha de 31 de mayo de 2025 "se detectó un incidente de seguridad en el sistema de gestión de ausencias del alumnado, comprometiendo los datos personales que pudieran estar en dicha base de datos", circunstancia por la cual pudieron verse afectadas todas las personas que en calidad de padre, madre, tutor/a o alumno/a estuvieran incluidos en esa fecha, en el sistema de gestión de ausencias de la comunidad educativa de Castilla y León. (Acceso en la web https://www.incibe.es/ciudadania/avisos/la-consejeria-de-educacion-informa-sobre-una-filtracion-de-datos-de-la-comunidad).

(por ejemplo, clases online), o del gran número de redes wifi públicas para facilitar el acceso del alumnado y del profesorado. La escasa conciencia de riesgo de los usuarios es, asimismo, un factor decisivo.

Mientras estuvo en vigor la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, no todos los ficheros de datos debían cumplir las mismas medidas de seguridad. Dichas medidas se clasificaban en tres niveles: básico, medio y alto atendiendo a la naturaleza de la información tratada, la mayor o menor necesidad de garantizar la confidencialidad y la integridad de la información.

Con carácter general todos los ficheros manejados por los centros de enseñanza que contenían datos de carácter personal debían adoptar las medidas de seguridad calificadas como de nivel básico, si bien todos aquellos ficheros en los que se contenían datos de salud (por ejemplo, en los ficheros en los que se guardaba información sobre absentismo del personal docente, o sobre enfermedades de los alumnos/as que y que debían tenerse en cuenta para la prestación del servicio del comedor, etcétera), debían implantarse medidas de seguridad de nivel alto.

En nuestro país, actualmente, la LOPDP de 2018 (Disposición Adicional 1ª), se remite a lo dispuesto en el RGPD de 2016 (art. 25), y al llamado Esquema Nacional de Seguridad[53] que incluirá las medidas que deban implantarse en caso de tratamiento de datos personales para evitar su pérdida, alteración o acceso no autorizado.

El RGPD no distingue, como sucedía con anterioridad entre los niveles de los ficheros, sino que especifica que se apliquen medidas de seguridad teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos para los derechos y libertades de las personas físicas (art. 25.1)[54].

[53] Regulado por Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (BOE de 4 de mayo de 2022).
[54] Tomar en consideración el estado de la técnica para garantizar un adecuado nivel de seguridad parece lógico y razonable, pero si se aplica de forma prioritaria el criterio del coste de aplicación, a la par que se rebaja el nivel de riesgo para los derechos y libertades de los ciudadanos de los datos existentes en los centros docentes, podemos generar importantes brechas de seguridad y vulnerabilidades.

El nuevo RGPD habla de “medidas técnicas y organizativas apropiadas” para garantizar un nivel de seguridad adecuado al riesgo, pero no concreta qué tipo de medidas deben aplicarse.

El RGPD, bajo el principio de responsabilidad proactiva (art. 5.2), exige al responsable del tratamiento que aplique las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el Reglamento.

El RGPD propone como mecanismos efectivos de verificación del cumplimiento la adhesión a códigos de conducta o a mecanismos de certificación (art. 42).

Por tanto, lo que el RGPD exige es que los responsables del tratamiento tengan una actitud consciente, diligente y proactiva del tratamiento de los datos, pudiendo demostrar, si llegara el caso, las medidas de seguridad aplicadas.

Por último, y para cerrar definitivamente este apartado, es preciso advertir que otra de las novedades relevantes que ha impuesto el RGPD al responsable del tratamiento es la obligación de notificar las violaciones de seguridad de los datos. Es decir, el responsable del tratamiento de los datos deberá notificar a la autoridad competente (AEPD en España) cualquier brecha o violación de seguridad que se haya producido, en el plazo máximo de 72 horas desde que tenga conocimiento la misma (Considerando 85 y art. 33 del RGPD).

Además, si la brecha implica un riesgo para los interesados, también se les deberá notificar a ellos (art. 34 RGPD).

5. Jurisprudencia y resoluciones relevantes

Si ilustrativa resulta para conocer el régimen legal aplicable la normativa en vigor, no lo es menos la jurisprudencia, es decir, el modo en el que, las resoluciones de los tribunales, hace aplicación de la normativa a los casos concretos.

5.1 Jurisprudencia española

Si bien ya se hizo referencia a diversas sentencias de nuestro TC en relación con el art. 18 de la CE de 1978[55], no debemos obviar las resoluciones de otros órganos jurisdiccionales en las que se han pronunciado sobre asuntos relativos al uso de sistemas de IA, u otros relevantes para la protección de datos personales, como puede suceder en los casos de uso de cámaras de videovigilancia, y la consiguiente captación de imágenes identificativas y/o de datos biométricos de identificación.

Así, por ejemplo, la Sentencia del Tribunal Superior de Justicia de la Comunidad de Madrid (TSJM) nº 1082/2010[56], de 10 de diciembre, relativa al conflicto entre las medidas de videovigilancia, los derechos fundamentales en el ámbito de centros de educación secundaria, y las afecciones que pueden causar a los trabajadores del centro y al alumnado.

En el FJ 4º de dicha sentencia se expresa que,

> en relación con la vulneración de los derechos fundamentales expresados para la instalación de los sistemas de cámaras o videocámaras, será necesario ponderar los bienes jurídicos protegidos (…) Toda instalación deberá respetar el principio de proporcionalidad, lo que, en definitiva, supone, siempre que resulte posible, adoptar otros medios menos intrusivos para la protección de los datos de carácter personal, con el fin de prevenir interferencias injustificadas en los derechos y libertades fundamentales. En consecuencia, el uso de cámaras o videocámaras no debe suponer el medio inicial para llevar a cabo sus funciones por las Administraciones Públicas, debiéndose valorar la utilización de estos sistemas en atención a su proporcionalidad en relación con el fin perseguido.

No obstante, tras un ponderado razonamiento jurídico, el TSJM llega a las siguientes conclusiones sobre el caso concreto:

> Este juicio de proporcionalidad tratándose de centros educativos públicos de Enseñanza Secundaria Obligatoria, no ofrece duda que en los tiempos actuales

[55] Véanse las SSTC 254/1993, de 20 de julio, 292/2000, de 30 de noviembre, o 76/2019, de 22 de mayo de 2019, entre otras.
[56] Recurso 644/2009, ECLI: ES:TSJM:2010:18374.

concurren más ventajas y beneficios que inconvenientes en la instalación de videocámaras en pasillos (no en las aulas), ya que se utilizan: a) como medida preventiva y disuasoria, b) como instrumento de identificación de aquellas personas que privan de sus derechos a la gran mayoría de la comunidad educativa, c) no se pretende almacenar imágenes sino garantizar los derechos de la mayoría y d) disminuir los gastos por desperfectos.

Una sentencia relevante y muy reciente, aunque no haga referencia específica en este caso al ámbito educativo, pero cuya doctrina puede ser igualmente aplicable al mismo, puede ser la Sentencia 1119/2025, de 11 de septiembre, del Tribunal Supremo (TS)[57] en relación con la posibilidad de acceso al código fuente, es decir, al lenguaje utilizado para crear un sistema de IA o, en su caso, a los modelos de IA capaces de generar código fuente, código que en unos casos puede ser abierto o accesible al público en general, incluso modificable, pero en otros no.

Pues bien, en aquellos supuestos en los que un programa o un sistema de IA adopta decisiones automatizadas, sin intervención humana, el conocimiento del código fuente, que determina esas decisiones, puede ser relevante para conocer los posibles sesgos discriminatorios. Por ello, la sentencia hace referencia a actuaciones automatizadas de la Administración en el ejercicio de sus competencias, a través de las cuales se adopta una decisión con evidente impacto en los derechos de los ciudadanos (por ejemplo, adjudicación de plazas escolares en centros docentes).

Dicha sentencia, con amparo en el art. de la Ley 15/2022, de 12 de julio, integral para la igualdad de trato y la no discriminación, que favorece la transparencia de los algoritmos empleados en la toma de decisiones por las Administraciones Públicas, reconoce el derecho de la parte demandante en su calidad de interesada, a acceder al código fuente de la aplicación informática utilizada para dicha toma de decisiones.

Por el contrario, la Sentencia de la Audiencia Nacional (SAN), de 22 de octubre de 2024[58], desestima la petición de acceso a la información solicitada a la Consejería de Educación y Juventud de la Comunidad de Madrid, en relación con el código fuente

[57] Recurso 7878/2024; ECLI:ES:TS:2025:3826.
[58] Recurso 49/2023; ECLI: ES:AN:2024:5981. La Sentencia se posiciona en contra del parecer del Consejo de Transparencia y Buen Gobierno (CTBG) de 19/11/2021, con referencia RT/0253/2021, que estima la reclamación de acceso a la información solicitada por constituir información pública en virtud de la Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno.

de la aplicación informática utilizada para el sorteo de tribunales, asociado a procesos selectivos en materia educativa.

Considera que dicho código está amparado por el derecho a la propiedad intelectual, y ello a pesar de que la titularidad de dicho programa corresponda a una Administración pública, al entender que su cesión a un tercero puede generar vulnerabilidades al sistema de información y propiciar ataques y usos indebidos.

5.2 Jurisprudencia europea (TJUE)

En relación con la consideración como datos personales de las respuestas por escrito de un examen realizadas por la persona examinada, aspirante en un examen profesional, y las anotaciones del examinador en relación con dichas respuestas, puede verse la Sentencia del TJUE de 20 de diciembre de 2017 (caso C-434/16, Peter Nowak).

El pleito parte de la negativa del Comisario de Protección de Datos de Irlanda a permitir al Sr. Nowak el acceso al escrito corregido de un examen en el que este participó como aspirante, negativa basada en el argumento legal de que, según la citada autoridad, los datos allí contenidos no eran de carácter personal.

Pues bien, el TJUE, apoyándose en la normativa europea vigente en aquel momento[59], considera que “las respuestas por escrito proporcionadas por un aspirante durante un examen profesional y las eventuales anotaciones del examinador referentes a dichas respuestas son datos personales”.

El TJUE (cuestión prejudicial 39), considera en relación con las respuestas y anotaciones del examinador que,

> el éxito o el fracaso del aspirante en el examen en cuestión, puede tener efectos en sus derechos e intereses, ya que, por ejemplo, puede condicionar sus oportunidades de acceder a la profesión o empleo al que aspira o influir en esas oportunidades.

[59] En este caso, la normativa aplicable era el artículo 2, letra a), de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

Cierto es que no se está aplicando este criterio a un examen corregido por un sistema de IA, pero igualmente podría hacerse extensivo quizás el criterio, tanto al conocimiento del resultado obtenido por el aspirante como a la publicidad del algoritmo utilizado para la corrección de las pruebas, en justa equivalencia a las anotaciones realizadas por un examinador para evaluar una prueba objetiva.

5.3 Resoluciones internacionales

Pero quizás las resoluciones más estrechamente vinculadas con el uso de IA y la protección de datos en el ámbito educativo internacional hayan sido las de las distintas autoridades europeas de protección de datos[60] y en especial, y por estudiar simplemente dos casos concretos, la alemana y la francesa, resoluciones en las que se denunciaban graves problemas de privacidad derivados del uso de los paquetes de Office 365[61], al no cumplir con lo dispuesto en el RGPD.

En el primero de los casos citados, las autoridades alemanas de protección de datos de los Estados federados de Hesse y Baden-Wurtemberg llegaron a prohibir el uso de Office 365[62] en colegios, al considerar que recopilaba de manera ilegítima datos de usuarios.

En concreto, y de acuerdo con un estudio posterior realizado por la Conferencia de Autoridades de Protección de Datos de los Estados federados alemanes (DSK)[63], se llegó a la conclusión de que los productos de Office 365 basados en la nube incumplían lo dispuesto en el RGPD en los siguientes aspectos:

- Ausencia de un interés legítimo para la obtención de datos personales, amparado en la expresión “fines comerciales legítimos”, expresión que adolece

[60] Así por ejemplo, en enero de 2022, la Autoridad de Protección de Datos de Austria decidió que el uso de Google Analytics infringía el RGPD; en febrero de 2022, el Gobierno holandés publicó una Evaluación del Impacto de la Protección de Datos (DPIA) en la que se evaluaban los riesgos de protección de datos del uso profesional de Microsoft Teams en combinación con OneDrive, SharePoint Online y el Directorio Activo de Azure; y en agosto de 2022, la Agencia de Protección de Datos de Dinamarca (DPA), prohibió el uso de Google Workspace en las organizaciones del sector público.

[61] Office 365, anteriormente conocido como Microsoft 365 es una plataforma o servicio por suscripción basada en la nube que ofrece aplicaciones como Word, Excel, PowerPoint, Outlook y Teams, junto con almacenamiento en la nube (OneDrive).

[62] La IA de Office 365 se refiere a Microsoft 365 Copilot, una herramienta de inteligencia artificial que integra modelos de lenguaje avanzados y los datos de la organización usuaria para ayudar en las tareas de las aplicaciones de Office. Funciona como un asistente inteligente que puede redactar correos, resumir documentos, crear presentaciones, analizar datos en Excel etc.

[63] Datenschutzkonferenz (DSK). Puede verse dicho informe (versión disponible únicamente en alemán) en https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/2022-11/26_ag_ms365_zusammenfassung_endg.pdf

de falta de concreción y no tiene una justificación adecuada en relación con clientes del sector público.

- Falta de transparencia, claridad y precisión en el lenguaje empleado en la contratación.
- Inseguridad de los datos, por falta de aplicación de medidas técnicas, organizativas y de control apropiadas.
- Indefinición en relación con el tratamiento de datos, de tal manera que resulta complejo determinar en qué casos Microsoft asume el papel de responsable o el de encargado del tratamiento.
- Insuficiencia de la información facilitada por Microsoft a otros sujetos, al no alcanzar los mínimos establecidos por las Cláusulas Contractuales Tipo diseñadas por la Comisión Europea.

En el segundo caso, con fecha de 15 de noviembre de 2022, la Autoridad francesa de Protección de Datos (CNIL)[64] solicitó a través de una advertencia formal dirigida al Ministerio competente en materia de educación[65] el cese del uso de las versiones gratuitas de Office 365 y Google Workspace en los colegios y universidades.

La CNIL consideró que el uso gratuito de este servicio suponía un claro ejemplo de *dumping*[66] y competencia desleal, además de un grave problema de localización de los datos en la nube, en concreto en servidores de EE. UU, sin garantía de cumplimiento de las exigencias del RGPD.

6. Medidas legales, buenas prácticas y estrategias de cumplimiento en materia de protección de datos

Además del estricto cumplimiento de la normativa de protección de datos, y de las disposiciones impuestas por la misma, es posible adoptar una serie de medidas que implementen su eficacia.

Refiriéndonos a las medidas adoptadas por la normativa vigente en materia de protección de datos, podemos aludir a la figura del delegado de protección de datos

[64] Agencia gubernamental Comisión Nacional de Informática y de las Libertades (CNIL).
[65] Pregunta escrita nº 971, publicada en el Journal Officiel de la République Française el 30 de agosto de 2022 (p. 3866), y respuesta publicada asimismo en el Journal Officiel de la République Française con fecha de 15 de noviembre de 2022 (p. 5395). https://questions.assemblee-nationale.fr/q16/16-971QE.htm
[66] El *dumping* es una práctica de comercio desleal consistente en vender productos en un mercado extranjero a un precio inferior al de su coste de producción o al de su mercado de origen.

(DPD), a las evaluaciones de impacto en materia de protección de datos (EIPD), al necesario consentimiento informado para el tratamiento de datos personales o las medidas de privacidad desde el diseño y protección de datos por defecto, exigidas por el RGPD.

Si hacemos alusión a las medidas que permiten implementar esta protección, podemos citar actuaciones como la formación y concienciación del profesorado, y las buenas prácticas implementadas desde algunas instituciones como la AEPD o las propias Administraciones educativas.

6.1 Delegado de Protección de Datos (DPD)

Una de las novedades fundamentales incorporadas por la normativa vigente en la materia objeto de estudio, ha sido la figura del Delegado de Protección de Datos (*Data Protection Officer*).

Su regulación legal puede encontrarse tanto en el RGPD, que le dedica la sección 4ª del Capítulo IV (arts. 37 a 39), como en la LOPDP, en concreto en sus arts. 34 a 37.

El DPD es la persona encargada de asesorar a la empresa, entidad o Administración, y asume las competencias de coordinación y control del cumplimiento de la normativa, en materia de protección de datos.

Esta figura no es obligatoria para todas las organizaciones, pero necesariamente debe existir un DPD en las empresas públicas, las que tengan un tratamiento a gran escala, o las que recojan datos especialmente sensibles o relativos a condenas o infracciones penales.

A partir de esta sencilla premisa, cabe plantearse si es obligatorio contar con un delegado de protección de datos en cada centro docente, o basta con designar un único delgado para para todos los centros y órganos administrativos existentes dentro de su ámbito competencial.

Pues bien, la cuestión queda resuelta en los arts. 37.3 del RGPD y 34.1.b de la LOPDP.

El art. 37.3 RGPD dispone que “cuando el responsable o el encargado del tratamiento sea una autoridad u organismo público, se podrá designar un único delegado de protección de datos para varias de estas autoridades u organismos, teniendo en cuenta su estructura organizativa y tamaño”.

Por su parte el art. 34.1.b LOPDP 2018 dispone que,

> los responsables y encargados del tratamiento deberán designar un delegado de protección de datos en los supuestos previstos en el artículo 37.1 del Reglamento (UE) 2016/679 y, en todo caso, cuando se trate de las siguientes entidades: (…) b) Los centros docentes que ofrezcan enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación, así como las Universidades públicas y privadas”.

En la práctica, y dada la complejidad que podría presentar la alternativa de designar un delegado para cada centro docente, las Administraciones educativas han optado por la solución de designar un único delgado para todo su ámbito competencial, en el que se incluyen todos los centros docentes, organismos y unidades administrativas.

El DPD deberá ser designado con cualidades profesionales y, en particular, con conocimiento experto de la legislación y prácticas de protección de datos, y con la capacidad de cumplir con las tareas impuestas por el RGPD, es decir, debe acreditar conocimientos técnicos en la materia (arts. 37.5 RGPD y 35 LOPDP)

El Delegado puede elegirse entre personal existente en la organización del responsable de los Datos, aunque también cabe la posibilidad de cumplir las tareas a través de un contrato externo de servicios.

Entre las funciones encomendadas al delegado de protección de datos se encuentran, las siguientes (art. 39 RGPD):

- supervisar la implementación y aplicación de las políticas internas de protección de datos.
- Realizar formación al personal en materia de protección de datos.
- Organizar y coordinar las auditorías.

- Gestionar la información de los interesados y las solicitudes presentadas en el ejercicio de sus derechos.
- Velar por la conservación de la documentación.
- Supervisar la realización de la evaluación de impacto en protección de datos.
- Actuar como punto de contacto para la autoridad de control.

6.2 Evaluaciones de Impacto en Protección de Datos (EIPD)

De acuerdo con lo establecido en el art. 35.1 del RGPD la evaluación de impacto en protección de datos (EIPD) debe realizarse por parte del responsable del tratamiento (en nuestro caso las Administraciones educativas o las entidades titulares de los centros privados o concertados), con el asesoramiento del DPD, "cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas (…)."

Esa EIPD es especialmente relevante en supuestos en los que se realice la evaluación de aspectos personales a partir de un tratamiento automatizado de datos, y "sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente (…)"; y también, en aquellos supuestos de tratamiento de datos a gran escala relativos al

> "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 (*sic*) de una persona física" (art. 35.3 en relación con el 9.1 del RGPD).

Según el art. 35.7 RGPD,

> 7. La evaluación deberá incluir como mínimo:
> a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;
> b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;

c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y

d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

El RIA también incide en la necesidad de realizar estas EIPD en el uso de tecnologías que cuenten con sistemas de IA.

Así se pone de manifiesto en los Considerandos 34 (en relación con el uso de sistemas de identificación biométrica) y 96, especialmente en este último, para garantizar la protección de los derechos fundamentales frente a la utilización de sistemas de IA de alto riesgo por parte de organismos de Derecho público, o de las entidades privadas que presten servicios públicos, con cita específica de los ámbitos educativo, sanitario, de servicios sociales, vivienda y justicia.

La EIPD se regula asimismo en los arts. 5.2.b; 26.9; 27 y Anexo VIII del RIA.

De ellos, nos interesa especialmente el contenido del art. 27, que establece la evaluación de impacto relativa a los derechos fundamentales para los sistemas de IA de alto riesgo.

Dicho precepto establece la obligación de realizar una EIPD con anterioridad al despliegue de sistemas de IA de alto riesgo del anexo III, en relación con el art. 6.2, entre los que se incluyen los de educación y formación profesional.

La evaluación tiene como objetivo describir los procesos en los que se utilizará el sistema de IA y su consonancia con la finalidad prevista; detallar el periodo de tiempo durante el cual va a ser utilizado el sistema de IA y su frecuencia de uso; poner de manifiesto las categorías de personas o colectivos afectados y los riesgos o perjuicios específicos que les puedan afectar; identificar las medidas de supervisión humana necesarias según las instrucciones de uso; y especificar las medidas que será necesario adoptar en caso de que se haga efectivo el riesgo, incluidos los mecanismos de gobernanza interna y reclamación.

6.3 Políticas de consentimiento informado

El RGPD y la LOPDP han reforzado la necesidad de consentimiento de las personas interesadas para el tratamiento de sus datos personales.

El RGPD define el consentimiento en su art. 4.11 como “toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen”.

Por su parte, la LOPDP exige también el consentimiento inequívoco de los interesados para el tratamiento de sus datos (art.6).

Sin embargo, como novedad respecto de la derogada LOPD de 1999, el nuevo RGPD indica que para poder considerar que el consentimiento es inequívoco, deberá existir una declaración del interesado o una acción positiva que manifieste su conformidad. El silencio, las casillas ya marcadas o la inacción no constituirán prueba de consentimiento (Considerando 32 del RGPD).

Así pues, los consentimientos prestados con anterioridad a la entrada en vigor de la nueva normativa y que no reunían las condiciones exigidas actualmente por el RGPD debieron ser solicitados de nuevo.

Otra de las novedades importantes es el tratamiento de datos de menores. Desde mayo de 2018 no pueden ofrecerse servicios de la sociedad de la información a menores de 16 años sin el consentimiento paterno o del tutor legal, salvo que una ley nacional establezca una edad inferior que, en ningún caso, será inferior a 13 años. En España, la LOPDP 2018 establece, salvo excepciones legales, la posibilidad de recabar datos personales de mayores de 14 años sin necesidad de obtener el consentimiento de sus padres (art. 7.1 LOPDP 2018). No obstante, como ya se ha dicho con anterioridad, esta norma puede ser próximamente modificada y ampliarse la edad de consentimiento hasta los 16 años.

6.4 Privacidad desde el diseño y protección de datos por defecto

La privacidad desde el diseño y protección de datos por defecto[67], conocida en la terminología anglosajona como "*privacy by design"* y *"privacy by default"* es un doble requerimiento impuesto por el RGPD, al que se hace referencia en los Considerandos 78 y 108, y más concretamente en su art. 25:

> 1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.
>
> 2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.
>
> 3. Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 42 como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo.

Así pues, la privacidad desde el diseño exige que las medidas de privacidad y protección de datos se integren desde el momento inicial de diseño de cualquier

[67] La AEPD ha desarrollado una Guía de Privacidad desde el Diseño, una Guía de Protección de Datos por Defecto y un listado de medidas que pueden consultarse en el siguiente enlace: https://www.aepd.es/preguntas-frecuentes/2-tus-obligaciones-como-responsable-del-tratamiento/9-analisis-de-riesgos/FAQ-0224-que-es-la-proteccion-de-datos-desde-el-diseno-y-por-defecto

producto, servicio o sistema, de tal manera que la seguridad de los posibles usuarios quede garantizada desde ese primer momento.

Por su parte, la protección de datos por defecto supone que únicamente sean objeto de tratamiento los datos estrictamente necesarios, y que hubieran sido determinados en la etapa de diseño inicial. Es lo que se denomina como "principio de minimización", es decir, una actuación, fundamentalmente por parte del responsable del tratamiento, en virtud de la cual se recabe la mínima cantidad posible de datos, que la extensión del tratamiento sea también la mínima posible, que los datos se conserven el mínimo plazo indispensable, y que se otorgue la mínima accesibilidad a los datos recabados. Todo ello, además, sin que sea necesaria intervención alguna por parte de los interesados, para garantizar dicha protección.

6.5 Formación del profesorado y concienciación

Como bien sabemos, la formación permanente del profesorado es una herramienta indispensable para dar respuesta a los nuevos retos educativos que plantea la sociedad actual, para mejorar la calidad de la enseñanza, para el desarrollo profesional y satisfacción del docente y, sobre todo, en nuestro caso, para garantizar la capacidad de adaptación a los cambios tecnológicos y metodológicos impuestos por las nuevas tecnologías. Es pues necesaria una mejora de la competencia profesional de los docentes para lograr el objetivo de una enseñanza de calidad.

En este sentido, y centrándonos en los dos aspectos principales de este estudio, es evidente que resulta indispensable una adecuada formación del profesorado en el uso de sistemas de IA, y en los riesgos derivados del mismo, sobre todo en materia de protección de datos de todo el colectivo que interviene en el proceso de enseñanza y aprendizaje.

Así, por ejemplo, desde el INTEF se han puesto en marcha acciones de formación para "impulsar la integración responsable de la inteligencia artificial en la formación permanente del profesorado"[68].

[68] Este trabajo fue presentado en el Congreso Nacional de Buenas Prácticas en Formación Docente los días 22 y 23 de mayo de 2025 en Santiago de Compostela, como una propuesta innovadora y necesaria para el desarrollo profesional del profesorado en el contexto digital actual. Véase https://intef.es/Noticias/la-inteligencia-artificial-en-la-formacion-del-profesorado-un-compromiso-con-la-educacion-del-futuro/

Por su parte, el Ministerio de Educación, Formación Profesional y Deportes, publicó en 2024 una "Guía sobre el uso de la inteligencia artificial en el ámbito educativo" elaborada asimismo por el INTEF, y que fue presentada en unas jornadas desarrolladas bajo el título "Jornadas IA en educación"[69].

Las Administraciones educativas de las Comunidades Autónomas están planificando, asimismo, actividades formativas en este campo para el profesorado[70], aunque en algún caso se han propuesto o establecido medidas de control o restricción de dichas actividades con el objetivo, según se afirma, de garantizar la seguridad de uso[71].

Igualmente lo están haciendo también los sindicatos más estrechamente vinculados al ámbito de la educación.[72]

Vemos pues que se está realizando un importante esfuerzo en este terreno, pero que es preciso incidir no sólo en su utilidad pedagógica, sino también en el manejo adecuado de esta tecnología, y en los posibles riesgos derivados del mismo, para la concienciación tanto del profesorado, como del alumnado.

6.6 Implementación de buenas prácticas

Todas las medidas anteriormente citadas se están viendo implementadas, asimismo, con la propuesta directrices y de códigos de buenas prácticas, en especial desde las

[69] Para más información véase https://www.miteco.gob.es/es/ceneam/recursos/materiales/guia-sobre-el-uso-de-la-inteligencia-artificial-en-el-ambito-edu.html

[70] Así, a modo de simple ejemplo podemos citar el curso ofertado en febrero de 2025 por el CIFPA (Centro de Innovación para la FP de Aragón) para el profesorado de FP, que lleva por título "Uso eficaz de herramientas de IA generativa para docentes de FP, y se oferta en modalidad online y presencial (https://cifpa.aragon.es/cursos/htas-ia-docentesfp-125/); Asimismo, la Comunidad de Madrid promovió un curso en el mes de marzo de 2025 bajo el título "Introducción a la IA para uso docente en el ámbito de la formación profesional" (https://www.educa2.madrid.org/es/web/albor/presentacion/-/visor/introduccion-a-la-ia-para-uso-docente-en-el-ambito-de-la-formacion-profesional).

[71] Ha sido el caso, por ejemplo, de la Junta de Andalucía, ya que, con fecha de 9 de septiembre de 2025, la Dirección General de Innovación y Formación del Profesorado publicó unas Instrucciones para el desarrollo de Grupos de Trabajo del curso 2025-2026. En el apartado 7, página 2, se establecía lo siguiente: "Con el fin de preservar un entorno digital seguro, no se aceptarán actividades relacionadas con la IA en modalidades de autoformación. Esta medida temporal nos permitirá unificar criterios y establecer directrices y controles sólidos que promuevan un uso profesionalizado de la IA alineado con nuestro compromiso con la seguridad y la protección de datos".

[72] Véase, por ejemplo, ANPE, en Aragón, que ofrece en octubre de 2025 el curso online de 100 horas de duración titulado "inteligencia artificial en educación: Aplicaciones Prácticas para el Aula. Nivel inicial". (https://anpearagon.es/notices/197200/Curso-homologado.-Online.-100-horas.-INTELIGENCIA-ARTIFICIAL-EN-EDUCACI%C3%93N.-Aplicaciones-Pr%C3%A1cticas-para-el-aula.-Nivel-inicial); o CSIF, que oferta para noviembre de 2025 un curso también de 100 horas que lleva por título "Uso de la Inteligencia Artificial en la Enseñanza" (https://campuseducacion.csif.es/FCCCurso.aspx?IDAreaTematica=56&IDCurso=3740).

Administraciones e Instituciones implicadas, como puede ser la Comisión Europea o, en nuestro país, la AEPD.

Así, por ejemplo, la Comisión Europea hizo públicas en febrero de 2025 las denominadas "Directrices de la Comisión sobre las prácticas prohibidas en materia de inteligencia artificial establecidas por el Reglamento (UE) 2024/1689 (Ley de IA)"[73].

La AEPD por su parte, publicó, ya en 2017, el "Código de buenas prácticas en protección de datos para proyectos BIG DATA"[74], y en febrero de 2020 la guía que lleva por título "Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción"[75].

Igualmente, y a título de simple ejemplo, el Departament d'Educació de la Generalitat de Catalunya publicó en febrero de 2024 la guía titulada "La intelligència artificial en l'educació. Orientacions i recomanacions per al seu ús als centres"[76].

De la misma forma el Departamento de Educación del Gobierno Vasco ha editado en 2025 la "Guía para el uso de las inteligencias artificiales en el ámbito educativo"[77].

Los ejemplos serían prácticamente interminables.

7. Conclusiones

A partir del estudio anteriormente realizado cabe ofrecer las siguientes conclusiones:

Primera: El uso de los sistemas de IA se está consolidando en el ámbito educativo como una herramienta tecnológica muy destacada, que puede ser aprovechada no sólo en el proceso de enseñanza, aprendizaje y evaluación del alumnado, sino también en labores de análisis predictivo y gestión administrativa. Sin embargo, este

[73] Véase el contenido de dichas directrices en https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act y asimismo, centrándose en el campo educativa, en https://epale.ec.europa.eu/es/content/directrices-sobre-las-practicas-prohibidas-de-ia-en-educacion. La Comisión destaca entre las prácticas prohibidas el reconocimiento de emociones en entornos educativos, salvo en casos de uso médico o de seguridad. Considera que esta tecnología puede ser intrusiva y discriminatoria, afectando la privacidad, la dignidad humana y la libertad de pensamiento de docentes y estudiantes.
[74] Véase en https://www.aepd.es/guias/guia-codigo-de-buenas-practicas-proyectos-de-big-data.pdf
[75] Véase en www.aepd.es/guias/adecuacion-rgpd-ia.pdf
[76] Véase en https://projectes.xtec.cat/ia/general/orientacions-i-recomanacions-per-lus-de-la-intelligencia-artificial-als-centres-educatius/
[77] Véase en https://www.euskadi.eus/contenidos/documentacion/inn_doc_adi_artif/es_def/adjuntos/Guia-uso-de-IA-en-educacion_Euskadi.pdf

uso no está exento de riesgos, en especial, en relación con la protección de datos personales del alumnado y del personal de los centros docentes.

Segunda: La regulación vigente aplicable en el marco europeo en relación con el uso de sistemas de IA establece unos estándares bastante elevados en materia de protección de datos. Dicha regulación incluye, fundamentalmente, el Reglamento General de Protección de Datos de la UE (RGPD) de 2016, el Reglamento Europeo de Inteligencia Artificial (RIA) de 2024 y, en nuestro país, la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDP) de 2018.

Tercera: Los principales riesgos del uso de sistemas de IA en el ámbito educativo derivan de la utilización de datos sensibles de menores de edad, de la adopción de decisiones automatizadas y perfilado de datos, de la posible transferencia internacional de los datos obtenidos a terceros países sin un adecuado nivel de protección, de los sesgos discriminatorios con los que han sido entrenados o configurados los algoritmos, y de los posibles fallos o brechas de seguridad de las tecnologías utilizadas.

Cuarta: Tanto la jurisprudencia, como las resoluciones de los órganos competentes de diversos países europeos en materia de protección de datos, están realizando una importante labor de aplicación de la normativa vigente, anteriormente citada. En dicha aplicación se intenta dotar de transparencia al funcionamiento de los algoritmos utilizados para la toma de determinadas decisiones, y establecer límites estrictos en aquellos supuestos en los que es dudoso el respeto a los derechos de los ciudadanos.

Quinta: Además del estricto cumplimiento de la normativa vigente, es conveniente implementar las medidas de protección con otras actuaciones como la adecuada formación y concienciación del profesorado y del alumnado, o el fomento de buenas prácticas, promovidas desde las Administraciones públicas educativas.

Financiación

Sin financiación expresa

Conflicto de intereses

Ninguno

Normativa básica de referencia

- Constitución española de 1978. BOE nº 311, de 29-12-1978.
- Ley Orgánica 2/2006, de 3 de mayo, de Educación (LOE). BOE nº 106, de 4 de mayo de 2006. Modificada por Ley Orgánica 3/2020, de 29 de diciembre (LOMLOE), por la que se modifica la Ley Orgánica 2/2006, de 3 de enero de Educación. BOE nº 340, de 30-12-2020.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos -RGPD-). Diario Oficial de la Unión Europea (DOUE) de 4-5-2015.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDP). Boletín Oficial del Estado (BOE) nº 294, de 6-12-2018.
- Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024 por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial -RIA-). DOUE de 12-7-2024.

Otros documentos

- Instituto Nacional de Ciberseguridad (INCIBE) (2024). El uso de la Inteligencia artificial en el entorno educativo. https://www.incibe.es/menores/blog/el-uso-de-la-inteligencia-artificial-en-el-entorno-educativo
- Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) (2025). Marco de competencias para docentes en materia de IA. https://doi.org/10.54675/AQKZ9414
- Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) (2025). Marco de competencias para estudiantes en materia de IA. https://doi.org/10.54675/EKCU4552

- Instituto Nacional de Tecnologías Educativas y de Formación del Profesorado (INTEF). (2024). Guía sobre el uso de la Inteligencia Artificial en el ámbito educativo. https://www.miteco.gob.es/es/ceneam/recursos/materiales/guia-sobre-el-uso-de-la-inteligencia-artificial-en-el-ambito-edu.html
- Agencia Española de Protección de Datos (AEPD). (2021). Requisitos para Auditorías de Tratamientos que incluyan IA. https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/aepd-publica-guia-requisitos-auditorias-tratamiento-ia
- Agencia Española de Protección de Datos (AEPD). (2020). Adecuación al RGPD de tratamientos que incorporan Inteligencia Artificial. Una introducción. https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/la-aepd-publica-una-guia-para-adaptar-al-rgpd-los-productos-y

Referencias bibliográficas

Álvarez Aguilar, J. F. y Acisclos García, M. T. (2025). Usos prácticos de la inteligencia artificial en la Inspección educativa. *Revista Supervisión 21*, nº 77. Recuperado a partir de https://supervision21.usie.es/index.php/Sp21/article/view/878

Artigas Oliveras, C. (2024). Del Reglamento Europeo de la IA hacia la necesaria gobernanza global. *Revista de Privacidad y Derecho Digital*. Vol. 9, nº 34, págs. 21 a 25. Recuperado a partir de https://revista.proeditio.com/rpdd/issue/view/644

Boix Palop, A. (2020). Los algoritmos son Reglamentos: la necesidad de extender las garantías propias de las normas reglamentarias a los programas empleados por la Administración para la adopción de decisiones. *Revista de Derecho Público: Teoría y Método*. Vol. 1. Págs. 223 a 270. Recuperado a partir de https://www.revistasmarcialpons.es/revistaderechopublico/article/view/33

Cabezudo Vidal, N. (2023). Las sentencias Schrems I (2015) y Schrems II (2020) del Tribunal de Justicia de la Unión Europea y la protección de datos de carácter personal en las relaciones internacionales. *CEFLegal. Revista Práctica de Derecho*, 265, págs. 91 a 126. Recuperado a partir de https://doi.org/10.51302/ceflegal.2023.15785

Cámara Villar, G. (2024) Protección de datos e inteligencia artificial en perspectiva europea, en *El Estado constitucional democrático* (Manuel Aragón Reyes *et al*. Dir.)

Madrid, España: Centro de Estudios Políticos y Constitucionales. Págs. 441 a 458. Recuperado a partir de https://www.cepc.gob.es/publicaciones/monografias/el-estado-constitucional-democratico-libro-homenaje-javier-jimenez-campo

Castellanos Claramunt, J.(2020). La gestión de la información en el paradigma algorítmico: inteligencia artificial y protección de datos. *Revista Métodos de Información*, 11(21), págs. 59 a 82. Recuperado a partir de https://dx.doi.org/10.5557/IIMEI11-N21-059082

Cazurro Barahona, V. (2024). La regulación del derecho a la educación digital. *Revista de Educación y Derecho (Education and Law Review)*. II número extraordinario (Inteligencia artificial y educación superior). Universitat de Barcelona. Págs. 82 a 114. Recuperado a partir de https://revistes.ub.edu/index.php/RED/article/view/49174

Crespo Ramos, S. (2025). Aplicación de la inteligencia artificial para la optimización temporal en tareas docentes: un análisis del potencial de mejora en educación primaria y secundaria en España. Recuperado a partir de https://supervision21.usie.es/index.php/Sp21/article/view/879

De Marcos Fernández, A. M. (2024). Una doble historia de la inteligencia artificial: avance tecnológico y proceso de regulación en Europa. *Revista de Privacidad y Derecho Digital*. Vol. 9, nº 34, págs. 26 a 89. Recuperado a partir de https://revista.proeditio.com/rpdd/issue/view/644

Fuertes López, M. (2024). Usuarios de los sistemas de inteligencia artificial y sus obligaciones. *Revista de Privacidad y Derecho Digital*. Vol. 9, nº 34, págs. 121 a 171. Recuperado a partir de https://revista.proeditio.com/rpdd/issue/view/644

Galicia Mangas, F. J. (2019). Protección de datos y transparencia en los centros docentes. *Supervisión 21*, *53* (53). Recuperado a partir de https://supervision21.usie.es/index.php/Sp21/article/view/402

Gallego Rodríguez, P. (2025). El derecho constitucional a la educación y la IA generativa: propuestas para mitigar la exclusión digital educativa. *Revista Estudios de Deusto. Revista de derecho Público*, vol. 73, nº 1. Recuperado a partir de https://revista-estudios.revistas.deusto.es/article/view/3329

González de la Garza, L. M. (2024) inteligencia artificial y educación superior. Posibilidades, riesgos aceptables y limites que no se deben traspasar. *Revista de Educación y Derecho (Education and Law Review)*. II número extraordinario (Inteligencia artificial

y educación superior). Universitat de Barcelona. Págs. 115 a 145. Recuperado a partir de https://revistes.ub.edu/index.php/RED/article/view/49175

Jiménez Linares, M. J. (2024). Riesgos de los sistemas de inteligencia artificial generativa y el Reglamento de Inteligencia Artificial europeo. *Revista de Privacidad y Derecho Digital*. Vol. 9, nº 34, págs. 236 a 315. Recuperado a partir de https://revista.proeditio.com/rpdd/issue/view/644

Muruaga Herrero, P. (2024) ¿Y si utilizamos ChatGPT en los exámenes? *Revista de Educación y Derecho (Education and Law Review)*. II número extraordinario (Inteligencia artificial y educación superior). Universitat de Barcelona. Págs. 493 a 511. Recuperado a partir de https://revistes.ub.edu/index.php/RED/article/view/49202

Paredes Gallardo, C. (2024) Aplicación de la inteligencia artificial en el ámbito educativo. Análisis de buenas prácticas y recomendaciones. *Revista de Educación y Derecho (Education and Law Review)*. II número extraordinario (Inteligencia artificial y educación superior). Universitat de Barcelona. Págs. 512 a 539. Recuperado a partir dehttps://revistes.ub.edu/index.php/RED/article/view/49204

Razquin Lizarraga, M. M. (2024). Sistemas de IA prohibidos, de alto riesgo, de limitado riesgo, o de bajo o nulo riesgo. *Revista de Privacidad y Derecho Digital*. Vol. 9, nº 34, págs. 172 a 235. Recuperado a partir de https://revista.proeditio.com/rpdd/issue/view/644

Rivero Ortega, R. (2024). Obligaciones de los proveedores de sistemas de IA. *Revista de Privacidad y Derecho Digital*. Vol. 9, nº 34, págs. 90 a 120. Recuperado a partir de https://revista.proeditio.com/rpdd/issue/view/644

Sánchez Barrilao, J. F. (2023). Inteligencia artificial y fuentes del Derecho. *Revista de Derecho Constitucional Europeo*, nº 39, págs. 135 a 172. Recuperado a partir de https://www.ugr.es/~redce/REDCE39/articulos/06_Barrilao.htm

Tébar Cuesta, F. (2020). Inteligencia artificial e inspección de educación. Reorganizar el servicio de Inspección de educación (SIE) para el siglo XXI. *Revista Supervisión XXI* (57) 1-22. Recuperado a partir de https://supervision21.usie.es/index.php/Sp21/article/view/482/891