4. Marco legal

4.1 Reglamento Europeo IA

Introducción

El pilar central de la normativa europea es el Reglamento (UE) 2024/1689, conocido como la Ley de Inteligencia Artificial (AI Act). Este documento representa la primera ley integral sobre IA en el mundo y establece las reglas de juego para cualquier sistema que se comercialice o utilice en territorio comunitario.

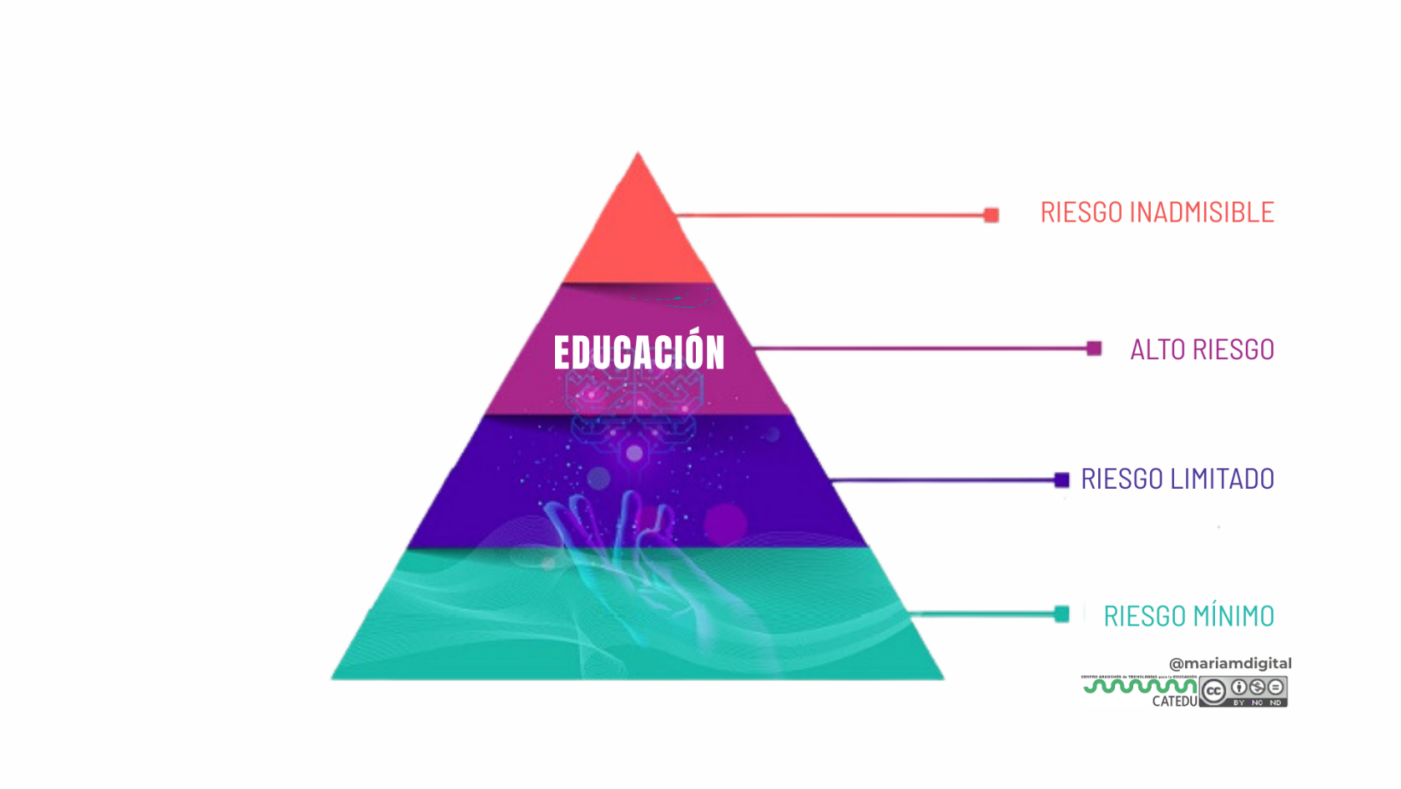
Tiene por objeto fomentar el desarrollo y la adopción de sistemas de IA **seguros** y **fiables** en todo el mercado único de la Unión Europea, tanto en el sector privado como en el público, garantizando al mismo tiempo la salud y la seguridad de los ciudadanos de la UE y el respeto de los **derechos fundamentales.**

La Ley de IA entrando en vigor (María de Mingo + Gemini)

Aunque ya ha ido apareciendo a lo largo de los capítulos de este curso, es necesario hacer zoom out para conocer tanto algunas cuestiones generales, como otras que afectan al sector educativo.

Niveles de Riesgo

En este Reglamento se establece una **clasificación de los sistemas de IA en función del riesgo** que suponen para la sociedad. Para la formación docente, es imperativo desglosar cómo este reglamento clasifica los sistemas de IA, ya que la educación ha sido designada como un ámbito de "alto riesgo" en algunos de sus puntos. Cuanto mayor sea el riesgo de causar daños a la sociedad, más estrictas serán las normas, culminando con la prohibición en aquellos casos que hayan sido clasificados como riesgo inadmisible o inaceptable.



Pirámide AI Act - Niveles de riesgo

Riesgo inadmisible - Prácticas prohibidas

Todos los sistemas de IA considerados una clara amenaza para la seguridad, los medios de subsistencia y los derechos de las personas son clasificados como Riesgo inadmisible y están prohibidos. El Reglamento **prohíbe** las siguientes prácticas de IA con un nivel de riesgo inaceptable:

- **Técnicas subliminales o engañosas** para manipular el comportamiento de individuos o grupos, mermando su capacidad para tomar decisiones con conocimiento de causa y causando un daño potencial.
- **Explotación de vulnerabilidades** basadas en la edad, la discapacidad o las situaciones socioeconómicas para manipular a individuos o grupos, con el consiguiente perjuicio potencial.

- **Puntuación social**, evaluando o clasificando a las personas en función de su comportamiento o características, lo que da lugar a un trato injusto no relacionado con el contexto en el que se recogieron los datos o de manera desproporcionada a la gravedad del comportamiento; por ejemplo a la hora de acceder a un empleo.
- **Evaluación del riesgo criminal**, predicción de la probabilidad de cometer un delito basándose únicamente en perfiles o rasgos de personalidad, excepto en investigaciones criminales objetivas y basadas en hechos.
- **Obtención de bases de datos de reconocimiento facial** a partir de Internet o de cámaras de seguridad sin un objetivo específico.
- **Inferencia de emociones en áreas sensibles,** como lugares de trabajo o instituciones educativas, a menos que se utilice con fines médicos o de seguridad.
- **Categorización biométrica** basada en datos para inferir atributos sensibles como raza, religión u opiniones políticas, excepto para su uso legal en el cumplimiento de la ley.
- **Identificación biométrica en tiempo real en público por parte de las fuerzas de seguridad**, a menos que sea estrictamente necesario para situaciones concretas (por ejemplo, encontrar a personas desaparecidas, prevenir amenazas inminentes o identificar a sospechosos de delitos graves). Esto debe seguir procedimientos legales estrictos, incluida la autorización previa, un alcance limitado y salvaguardias para proteger los derechos y libertades.

Alto riesgo - Educación

La designación de la educación como sector de alto riesgo se debe a que las **decisiones tomadas por una IA** en este ámbito pueden **determinar el curso de la vida académica, profesional y personal** de una persona. No obstante, **no todos los usos de la IA en educación se clasifican como de alto riesgo**, ya que esta categoría se aplica principalmente a aquellos sistemas que intervienen en decisiones relevantes como la admisión o la evaluación del alumnado.

> Son considerados de **alto riesgo** los sistemas de IA utilizados para determinar el **acceso** o admisión a centros, **evaluar** resultados del aprendizaje, valorar el nivel educativo adecuado o **supervisar** comportamientos prohibidos durante los exámenes.

Estos sistemas de IA deben cumplir con los **requisitos estipulados** en los artículos 8 al 17 de la ley, es decir, están sujetos a **obligaciones estrictas** antes de que puedan comercializarse:

- Sistemas adecuados de evaluación y mitigación de riesgos
- Alta calidad de los conjuntos de datos que alimentan el sistema para minimizar los riesgos de resultados discriminatorios
- Registro de la actividad para garantizar la trazabilidad de los resultados
- Documentación detallada que proporcione toda la información necesaria sobre el sistema y su finalidad para que las autoridades evalúen su cumplimiento
- Información clara y adecuada al implementador

- Medidas adecuadas de supervisión humana
- Alto nivel de robustez, ciberseguridad y precisión

Casos alto riesgo en Educación y FP

En cuanto a la protección de los derechos fundamentales y el **uso de sistemas de IA de alto riesgo**, la Ley IA dice que:

> Antes de que un sistema de IA de alto riesgo sea desplegado por entidades que prestan **servicios públicos**, debe **evaluarse su impacto sobre los derechos fundamentales** (art.27)**.** Los sistemas de IA de alto riesgo y las entidades que los utilicen deben **registrarse** en una **base de datos de la UE** (agosto 2027).

Además de los proveedores y distribuidores de sistemas de IA y de las entidades, los **centros educativos** y **docentes** podemos ser identificados como **responsables del despliegue** bajo el Reglamento Europeo de IA, por lo que también adquirimos responsabilidades si utilizamos sistemas de IA en los casos mencionados anteriormente, clasificados como de alto riesgo.

Algunas de las principales responsabilidades a la hora de desplegar estos sistemas son:

- **Uso conforme a las instrucciones:** adoptar medidas técnicas y organizativas adecuadas para garantizar que utilizan los sistemas siguiendo las **instrucciones de uso** facilitadas por el proveedor.

- **Supervisión humana:** obligación de encomendar la supervisión de estos sistemas a personas físicas que posean la **competencia, formación y autoridad necesarias** para vigilar su funcionamiento y prevenir riesgos.
- **Vigilancia y reporte:** vigilar el funcionamiento del sistema y, en caso de considerar que presenta un riesgo o detectar un **incidente grave**, deben informar inmediatamente al proveedor o distribuidor y a la autoridad de vigilancia del mercado, suspendiendo el uso del sistema si es necesario.
- **Calidad de los datos de entrada:** asegurarse de que los datos que introducen en el sistema sean pertinentes y suficientemente representativos, en la medida en que tengan control sobre ellos.
- **Conservación de registros:** obligación de conservar los **archivos de registro (logs)** generados automáticamente por el sistema durante al menos **seis meses**, para permitir la trazabilidad del funcionamiento si fuera necesario.
- **Deber de información:** si toman decisiones o ayudan a tomarlas basándose en estos sistemas, deben **informar a las personas físicas,** de que están siendo objeto del uso de una IA de alto riesgo.
- **Evaluación de impacto:** En el caso de centros que sean organismos de Derecho público o entidades privadas que presten servicios públicos, deben realizar una **evaluación de impacto relativa a los derechos fundamentales** antes de poner el sistema en funcionamiento.

Además, el reglamento subraya la importancia de la **alfabetización en materia de IA**, instando a que los responsables del despliegue garanticen que su personal tenga un nivel de conocimientos suficiente para operar estos sistemas de forma informada y segura.

Riesgo limitado y mínimo

> Se considera que todos los demás sistemas de IA presentan un **riesgo limitado**, por lo que el Reglamento no introduce más normas.

Evaluación y revisión

La Comisión evalúa cada año la necesidad de modificar la lista de usos de alto riesgo de la IA y la lista de prácticas prohibidas. Antes del **2 de agosto de 2028**, y cada cuatro años a partir de entonces, la Comisión evaluará e informará sobre lo siguiente:

- la adición o ampliación de la lista de **categorías de alto riesgo.**
- las modificaciones de la lista de sistemas de IA que requieren medidas de **transparencia adicional.**
- las modificaciones para mejorar **la supervisión y la gobernanza**.

Entrada en vigor

La **Ley Europea de Inteligencia Artificial** (AI Act) tiene una **entrada en vigor gradual**. Las fechas clave son:

- **1 de agosto de 2024**: la ley **entra formalmente en vigor** tras su publicación en el Diario Oficial de la UE el 12 de julio de 2024.
- **2 de febrero de 2025**: empiezan a aplicarse las **prohibiciones de ciertos usos de IA** y las **obligaciones de alfabetización en IA**.
- **2 de agosto de 2025**: entran en aplicación las normas para **modelos de IA de propósito general (GPAI)** y parte del sistema de gobernanza.
- **2 de agosto de 2026**: **la mayor parte de las obligaciones del AI Act empieza a aplicarse** y comienza su aplicación general en los Estados miembros.
- **2 de agosto de 2027**: se aplican los requisitos para algunos **sistemas de IA de alto riesgo integrados en productos regulados** (por ejemplo, ciertos dispositivos o maquinaria).

Timeline AI Act (María de Mingo+Gemini)

> En la **Plataforma única de información sobre la ley de IA** dispones de herramientas para consultar y navegar fácilmente por la ley además de realizar consultas. Para acceder pincha aquí.

Aquí puedes consultar también un resumen general de la ley.

Resumen

La **Ley de IA** establece requisitos jurídicamente vinculantes para los sistemas de IA y obligaciones para los operadores (incluidos proveedores y desplegadores). Una vez que la AI Act entre plenamente en vigor, las instituciones educativas, cuando sean consideradas usuarias de herramientas de IA de **alto riesgo**, podrán basarse en la evaluación de conformidad realizada por el proveedor, al tiempo que deberán cumplir sus propias responsabilidades como desplegadores conforme a la normativa.

Para los centros educativos y el profesorado las **directrices éticas** mencionadas en el capítulo anterior pueden proporcionar una mayor claridad sobre lo que exige la legislación en la práctica cotidiana. Además es importante hacer hincapié en la **alfabetización en IA** por parte de profesorado y alumnado; puedes recordar y consultar los marcos existentes aquí.

Por otro lado, las **directrices legales estrictas** que los docentes deben conocer para evitar riesgos son:

- **Prácticas prohibidas:** Está prohibido el uso de sistemas de IA para **inferir o detectar emociones** del alumnado en centros educativos, salvo por motivos de seguridad o médicos.
- **Sistemas de alto riesgo:** Las herramientas usadas para **evaluar resultados de aprendizaje,** monitorear el **comportamiento en exámenes**, determinar **admisiones** o seguir el **progreso del estudiante** se consideran de **alto riesgo** y requieren una supervisión humana y gobernanza de datos muy estricta.

Ejemplos concretos en el ámbito educativo

En *Orientaciones para integrar la IA en centros educativos del Área de Formación del Profesorado del INTEF* nos proporcionan los siguientes ejemplos:

- ⚠ **APLICACIÓN DE CORRECCIÓN AUTOMÁTICA DE EXÁMENES**: El proveedor de la IA (la empresa que vende, por ejemplo, un software de auto-corrección de exámenes) deberá cumplir ciertos requisitos: entrenar el modelo con datos fiables y no discriminatorios, validar su exactitud, documentar su funcionamiento y pasar una evaluación de conformidad.

El centro educativo que lo use tendrá que desplegarlo de forma responsable: seguir las instrucciones de uso, supervisar los resultados y contar con personal preparado para intervenir. Estas herramientas nunca deberían funcionar de modo totalmente autónomo sin supervisión docente. Por ejemplo, un software de IA que califica exámenes tipo test o incluso ensayos escritos (por ejemplo, asignando puntuaciones a redacciones de lengua). Esto es posible y legal, siempre y cuando se haga con supervisión y garantías de equidad. Además, los resultados de la IA no deberían emplearse para asignar calificaciones definitivas ni orientaciones en el aprendizaje.
En la práctica, un profesor podría usar la IA para agilizar la corrección, pero revisando las respuestas donde la IA presente dudas. La IA puede dar un *feedback* inicial y el docente confirma o ajusta la nota. No sería aceptable delegar al 100% la nota final en la IA sin intervención humana. Con un uso adecuado, la corrección automática puede ahorrar tiempo en evaluaciones diarias. Siempre se debe ofrecer al alumnado la posibilidad de revisión humana de sus calificaciones si lo solicita.

- ⚠ **VIGILANCIA DE EXÁMENES CON IA**: Durante la pandemia se popularizaron sistemas de *proctoring* remoto que usan IA para vigilar exámenes *online* mediante la cámara del ordenador. Estos programas detectan comportamientos como apartar la mirada constantemente, sonidos ambientales, presencia de otra persona en cámara, etc., y alertan de posible copia.
  Bajo la Ley de IA, esta práctica se puede emplear, pero es considerada de alto riesgo, lo que impone condiciones estrictas. Por ejemplo, la empresa proveedora del software debe garantizar que el sistema ha sido entrenado para diferentes características físicas (que no penalice injustamente, por ejemplo, a estudiantes con tics nerviosos o discapacidades) y minimizar falsos positivos. El centro educativo, por su parte, debe informar previamente al alumnado de que se usará esta tecnología y debe haber personal supervisando las alertas de la IA en tiempo real o a posteriori. Es decir, si la IA señala que un estudiante concreto "podría estar copiando", un supervisor humano debe revisar la grabación o evidencias antes de acusar o sancionar. No sería aceptable anular automáticamente el examen de un estudiante solo porque la IA lo marcó, sin verificación humana. Además, ciertas funciones están vetadas: por ejemplo, si el *proctoring* intentara analizar las expresiones faciales del alumno/a para saber si está nervioso o mintiendo, eso entraría en reconocimiento emocional, lo cual está prohibido. Igualmente, grabar continuamente al estudiante es invasivo, por lo que debe valorarse la proporcionalidad y cumplir con protección de datos. En definitiva: la vigilancia inteligente de exámenes es legal, pero bajo mucha cautela. De hecho, varios países de la UE ya han cuestionado estas herramientas por privacidad; el Reglamento refuerza que, de usarse, sea con todas las garantías para el alumno (información, supervisión humana, derecho a réplica).

- **PERSONALIZACIÓN DEL APRENDIZAJE**: Un escenario cada vez más común es usar IA para personalizar materiales educativos. Por ejemplo, un sistema de tutorización inteligente que adapte los ejercicios de matemáticas en función de los aciertos/errores del

estudiante, o plataformas de aprendizaje de idiomas que ajustan la dificultad según el progreso. Estas aplicaciones son legales y deseables, ya que pueden mejorar la atención a la diversidad en el aula. No se consideran de alto riesgo si la IA NO utiliza los resultados para orientar el proceso de aprendizaje. porque no están tomando decisiones definitivas sobre el alumnado, sino dando recomendaciones. El profesorado sigue teniendo control sobre el currículo y las evaluaciones formales. ⚠ El Reglamento impone algunas buenas prácticas: asegurar la transparencia y el conocimiento de la persona usuaria. Si un estudiante interactúa con un *chatbot* educativo o un tutor virtual, debe quedar claro que es una IA y no un humano real respondiendo. Muchos estudiantes jóvenes podrían pensar que hablan con un "profesor *online*", así que conviene aclararlo (muchas apps ya lo indican en sus términos, ahora será obligación legal hacerlo de forma accesible). Para el profesorado, usar IA en personalización implica revisar de vez en cuando las sugerencias del sistema, asegurarse de que los contenidos son adecuados al currículo oficial y que no introducen sesgos. Como estas herramientas de IA no deciden notas, ni accesos, el Reglamento solo les aplica obligaciones leves (transparencia). De hecho, se las considera de riesgo limitado, sujeto únicamente a informar a las personas usuarias finales que interactúan con IA, como mencionamos. Por tanto, un centro educativo podría implementar, por ejemplo, un asistente de ayuda con los deberes basado en IA sin necesidad de complejos trámites, más allá de cerciorarse de que el proveedor cumple la normativa y de avisar a la comunidad educativa de su uso. Personalizar no está prohibido; lo que activa alto riesgo es cuando el sistema evalúa resultados (o decide/condiciona itinerarios) con efectos relevantes. Entonces toca régimen de alto riesgo.

- **ANÁLISIS PREDICTIVO DEL RENDIMIENTO**: algunos centros educativos podrían usar sistemas de IA para predecir qué estudiantes necesitan refuerzo, analizando calificaciones previas, asistencias, etc. Siempre que esto se use como ayuda al docente y no para decidir automáticamente decisiones educativas importantes (calificaciones, expulsiones o repeticiones). Sería similar a emplear analítica de datos: identificar patrones para que luego un humano tome acciones pedagógicas. ⚠ La diferencia clave es si la IA reemplaza una decisión humana importante (no permitido sin cumplir estrictas condiciones) o si solo apoya o informa al humano (permitido).

- **IA PARA LABORES ADMINISTRATIVAS**: En tareas de administración, la IA es muy útil y no presenta mayores conflictos, siempre que se garantice una protección de los datos personales: por ejemplo, usar algoritmos para optimizar horarios de clase, rutas de transporte escolar, gestión de bibliotecas, planificación de espacios, etc., son usos internos que no afectan directamente a los derechos del alumnado. ⚠ La priorización automática de acceso a apoyos, becas o plazas es alto riesgo.

- **GENERACIÓN DE MATERIALES**: Usar un chatbot (como ChatGPT, Copilot, Gemini o Claude) para crear situaciones de aprendizaje, rúbricas o adaptar textos a diferentes niveles, siempre que el docente sea quien valide el contenido final está totalmente

permitido según esta ley. Si es el alumnado el que interactúa con el *chatbot*, debe estar informado de que está dialogando con un sistema de IA.

- **PROHIBIDO EL USO DE CÁMARAS PARA INFERIR EMOCIONES**: Un centro educativo NO puede instalar cámaras o micrófonos con IA para inferir estados emocionales del alumnado (atención, motivación, estrés…) con fines disciplinarios o de evaluación, excepto por motivos médicos o de seguridad muy específicos. Por ejemplo, si hubiese una herramienta para detectar signos de depresión o riesgo de autolesión en estudiantes concretos, podría argumentarse un fin médico/seguridad y quizá cabría (habría que ver caso por caso y otras leyes como protección de datos). Como norma general, analizar las emociones de los estudiante con IA para cualquier otro fin educativo es ilegal. Esto protege la intimidad y evita técnicas intrusivas poco fiables.

- **APLICACIÓN EDUCATIVA CON INFORMACIÓN SUBLIMINAL:** El uso de información subliminal o trucos manipuladores ocultos para enganchar a estudiantes en el uso de la aplicación estaría prohibido. Asimismo las aplicaciones que incitan al estudiante a comportarse de forma perjudicial para sí mismo o para otras personas.

> El Reglamento introduce obligaciones de información cuando pueda surgir un riesgo por falta de **transparencia en torno al uso de la IA**:
> - En algunos casos, el **resultado de la IA generativa debe estar visiblemente etiquetado,** como en el caso de los «deepfakes» y los textos destinados a informar al público sobre asuntos de interés público.
> - El resultado de la IA generativa debe marcarse como **generado por IA** de forma legible por máquina.
> - La IA diseñada para hacerse pasar por humanos (por ejemplo, un «chatbot») debe **informar al humano** con el que está interactuando.

> También es obligatorio respetar la legislación de la UE sobre **derechos de autor**.

Sin embargo, en el ámbito de la protección de datos, la ley ha de complementarse con el Reglamento General de Protección de Datos del que hablaremos a continuación.

4.2 Protección de datos

Tras haber analizado el marco que establece la Ley de Inteligencia Artificial de la Unión Europea (AI Act), es necesario abordar ahora el otro gran pilar normativo que regula el uso de la inteligencia artificial cuando implica el manejo de información personal: el **RGPD** (Reglamento General de Protección de Datos), que exige consentimiento explícito de uso de datos personales, seguridad de datos, notificaciones de brechas y otorga derechos de acceso, rectificación y supresión de los mismos (derecho al olvido).

En su artículo 8, el RGPD nos habla de las **condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información** y dice que

> el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como **mínimo 16 años**. Los Estados miembros podrán establecer por ley una edad inferior a tales fines, **siempre que esta no sea inferior a 13 años.**

En España este reglamento se complementa con la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (**LOPDGDD**), que adapta y desarrolla sus disposiciones en el contexto jurídico nacional. Juntos, estos instrumentos configuran el marco legal fundamental para garantizar que el uso de datos en entornos digitales y educativos respete los derechos y libertades de las personas.

Concretamente, en el artículo 92 de esta ley encontramos que:

> Los **centros educativos** y cualesquiera **personas físicas** o jurídicas que desarrollen **actividades en las que participen menores** de edad **garantizarán** la protección del interés superior del menor y sus derechos fundamentales, especialmente el derecho a la **protección de datos personales**, en la publicación o difusión de sus datos personales a través de servicios de la sociedad de la información.
>
> Cuando dicha publicación o difusión fuera a tener lugar a través de servicios de redes sociales o servicios equivalentes **deberán contar con el consentimiento** del menor (si es **mayor de 14 años**) o sus representantes legales, conforme a lo prescrito en el artículo 7 de esta ley orgánica.

> Los **datos personales** se refieren a cualquier información relacionada con una persona identificada o identificable.

En las directrices éticas de la Comisión Europea, podemos leer que, como responsables del tratamiento, las instituciones educativas deben comunicar de forma clara y accesible cómo procesan los datos personales (artículos 12-15 del RGPD), utilizando un lenguaje conciso y sencillo, especialmente cuando la información está dirigida a menores. El RGPD también exige realizar una **evaluación de impacto relativa a la protección de datos (EIPD o DPIA) antes de implementar sistemas**, incluidos los de inteligencia artificial, que puedan suponer un alto riesgo para los derechos y libertades de las personas (artículo 35).

Según la AEPD (Agencia Española de Protección de Datos), el **responsable del tratamiento de datos** son las administraciones educativas en el caso de los centros públicos y los propios centros educativos en los concertados o privados. El profesorado debe utilizar únicamente las aplicaciones, plataformas o servicios autorizados por dicho responsable y adaptar su uso al grado de desarrollo del alumnado. En caso de emplear herramientas o servicios distintos a los establecidos, el profesorado podría asumir la responsabilidad del tratamiento de los datos utilizados.

> Para más información sobre cuestiones relativas a la **privacidad y a la protección de datos de los menores** puedes acceder al Canal Joven de la AEPD. También puedes consultar "Responsabilidades y obligaciones en la utilización de dispositivos digitales móviles en la enseñanza infantil, primaria y secundaria" de la AEPD.

Como docentes, debemos saber que cualquier imagen o vídeo donde una persona sea identificable se considera un **dato personal**, incluso si se modifica o genera mediante **inteligencia artificial**. Al subir estas imágenes a una plataforma de IA, se produce una **pérdida de control,** que limita en la práctica el ejercicio de los derechos de acceso, supresión u oposición: el contenido pasa a manos de una empresa externa que puede conservarlo, crear copias ocultas o utilizarlo para sus propios fines sin que lo sepamos. Este riesgo existe aunque el uso sea puramente lúdico, como crear un avatar o aplicar un filtro, ya que el sistema analiza rasgos físicos y genera metadatos que permanecen en la red.

Además de estos riesgos, existen impactos visibles que pueden dañar gravemente a las personas, como la creación de escenas falsas que parecen reales, la suplantación de identidad o la generación de contenido íntimo sintético. El nivel de precaución debe ser máximo al trabajar con **menores de edad**, ya que una imagen aparentemente inocente procesada por IA puede derivar en situaciones de acoso, estigmatización o daños psicológicos en el entorno escolar.

Es fundamental entender que **tener acceso a una foto no da permiso** para transformarla con herramientas digitales. La protección de la privacidad de los estudiantes debe ser siempre la prioridad, por ello profundizaremos un poco más y hablaremos del Derecho de imagen en la próxima página.

4.3 Derecho de imagen

El derecho a la propia imagen está regulado por la Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar, y a la Propia Imagen.

> Toda persona tiene **derecho a decidir** sobre la **utilización** que se hace de **su imagen**. La imagen en el que una persona es identificada o identificable es un dato personal.

Como dice GVA, en el mundo actual, los derechos de imagen han tomado otra dimensión, y en consecuencia, tienen una gran importancia por las razones que se enumeran a continuación:

1. **Protección de la privacidad**. En un mundo en el que las imágenes y los vídeos se comparten y distribuyen con facilidad a través de las redes sociales y otros medios de comunicación, los derechos de imagen son esenciales para proteger la privacidad de las personas. Permiten a los individuos controlar el uso de su imagen y evitar su explotación sin su consentimiento.
2. **Protección de la reputación**. Estos derechos también son importantes para proteger la reputación de las personas. Si una imagen se utiliza de manera inapropiada o engañosa, puede afectar negativamente a su reputación. En estos casos, permiten a las personas tomar medidas legales para proteger su reputación y evitar la difusión de información falsa o engañosa.

La IA y el derecho de imagen (María de Mingo+Gemini)

> Como docentes es fundamental comprender que el **derecho a la imagen** protege no solo el aspecto físico, sino también la **voz, el nombre y cualquier rasgo identificativo** de una persona.

Al ser considerada un **dato personal**, la ley prohíbe captar, difundir o utilizar la imagen de alguien sin su **consentimiento expreso**, lo que significa que cada persona tiene el poder total de decidir si permite o no que se tome su foto o vídeo dentro o fuera del entorno educativo. Este derecho es permanente y debe respetarse siempre, ya que permite a cada individuo controlar el uso, difusión o publicación de su propia identidad.

Como dice **LeGardon**, todas las personas podemos decidir si autorizamos o no que nuestra imagen sea tomada por un tercero.
Se trata de un derecho imprescriptible que incluso las personas herederas pueden ejercer tras el fallecimiento de la persona titular del derecho de imagen, en lo referente a su “memoria”.

En el caso de los **menores de edad**, la protección es máxima y se exige siempre la **autorización por escrito de los padres o tutores legales**, pudiendo intervenir incluso la Fiscalía de Menores para asegurar su protección. Cualquier permiso otorgado **puede ser revocado en cualquier momento**; si una familia decide cambiar de opinión, la imagen debe dejar de usarse y ser retirada, aunque esto podría conllevar el pago de daños si la imagen ya forma parte de materiales editados. Existen excepciones muy limitadas, como cuando la imagen es secundaria en una noticia relevante

o se trata de cargos públicos en actos abiertos, pero estas nunca permiten el uso de la imagen para burlas o con fines comerciales sin permiso.

> Subir, reenviar a plataformas, redes o sistemas de IA, transformar o generar contenidos visuales a partir de la imagen de una persona supone un tratamiento de datos personales, con independencia de la finalidad perseguida o del carácter aparentemente trivial del uso.

En este mismo sentido y entendiendo que el **derecho a la imagen** protege **cualquier rasgo identificativo** de una persona, tal como dice la AEPD en su documento "Criterios para el tratamiento de datos personales en centros educativos", el profesorado debe prestar especial atención a los **contenidos de los trabajos de clase** que se publican o comparten en servicios digitales, utilizando únicamente los medios validados por el responsable del tratamiento de datos.

Asimismo, debería **transmitir esta misma prudencia al alumnado**, enseñándole el **valor de la privacidad propia y ajena**, y recordando que **no se deben realizar fotografías o vídeos de otros alumnos, profesores u otro personal del centro sin su consentimiento, y mucho menos difundirlos en redes sociales,** para evitar riesgos de violencia digital como el ciberacoso, el grooming, el sexting o la violencia de género. En relación con esta protección, la Ley Orgánica 8/2021 de protección integral a la infancia y la adolescencia frente a la violencia (LOPIVI) establece que todos los centros educativos en los que estudien menores de edad deben contar con una persona coordinadora de bienestar y protección del alumnado que, bajo la supervisión de la dirección del centro, promoverá la comunicación de las situaciones que impliquen un tratamiento ilícito de datos a las autoridades de protección de datos (artículo 35.1).

> Además, en la Guía para el uso de IA generativa en educación e investigación de la UNESCO(2024) se ha señalado que los **GPTs pueden contravenir leyes** como el Reglamento General de Protección de Datos de la Unión Europea (2016) o GDPR, especialmente el derecho de las personas a ser olvidadas, dado que actualmente es **imposible eliminar los datos** de alguien (o los resultados de esos datos) de un modelo GPT **una vez que ha sido entrenado.**

> Conviene recordar que también son **datos personales** los **resultados académicos** del alumnado y su número del expediente académico.

> Recomendamos encarecidamente la lectura de "***El uso de imágenes de terceros en sistemas de inteligencia artificial y sus riesgos visibles e invisibles***" (2026) de la

AEPD. Puedes acceder pinchando aquí.