

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 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.



Updated 2026-03-12 14:28:27 CET by Maria