

Grupo 1 - Cegados por la IA

Análisis de Privacidad y Cumplimiento Normativo

1. Marco normativo y preguntas clave

1.1. Afectación de la IA Act al proyecto

El proyecto Cegados Por La IA consiste en unas gafas inteligentes que utilizan inteligencia artificial para convertir las imágenes captadas por una cámara en descripciones orales en tiempo real, destinadas a personas con discapacidad visual.

Según el Reglamento Europeo de Inteligencia Artificial (IA Act), este sistema se clasificaría como una IA de **alto riesgo** debido a:

- Afecta directamente a los derechos fundamentales de las personas (accesibilidad y autonomía de usuarios con discapacidad).
- Procesa datos biométricos e información visual de terceros, es decir, puede implicar riesgos para la privacidad o la dignidad de las personas grabadas.
- Puede influir en el comportamiento o decisiones del usuario, al ofrecer descripciones que guían su percepción del entorno.

Como sistema de alto riesgo, el proyecto deberá cumplir con las exigencias de la IA Act, entre las cuales destacan:

- Documentación técnica y trazabilidad del sistema: descripción del modelo, su funcionamiento, datos utilizados para el entrenamiento y pruebas de sesgos.
- Supervisión humana efectiva: el usuario debe conservar siempre el control y poder desactivar o corregir las descripciones, mediante testeo pre-lanzamiento y con evaluación de uso real post-lanzamiento.
- Evaluación de conformidad y registro en la base europea de sistemas de IA de alto riesgo.
- Explicabilidad y transparencia: el usuario debe conocer cómo y por qué se generan las descripciones.

1.2. Aplicación del GDPR y la LOPDGDD

El sistema trata información que pueden considerarse datos personales según el Reglamento General de Protección de Datos (GDPR) y la Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de Derechos Digitales (LOPDGDD).

Sujetos afectados:

- Usuarios de las gafas: personas con discapacidad visual que utilizan el sistema.
- Terceros grabados: personas presentes en el entorno que podrían ser captadas por la cámara.

Tipos de datos tratados:

- Datos biométricos (rostros, rasgos faciales).
- Datos de localización (entorno físico, espacios visitados).
- Datos contextuales (acciones, objetos o personas descritas)

Bases legales para el tratamiento:

- Artículo 6.1.f del GDPR: interés legítimo del responsable del tratamiento en desarrollar una tecnología que mejore la accesibilidad.
- Artículo 9.2.g del GDPR: excepción para el tratamiento de datos sensibles con fines de interés público esencial y accesibilidad para personas con discapacidad.

1.3. Derechos y control de los usuarios

El usuario mantiene un control total sobre el tratamiento de sus datos y el funcionamiento del dispositivo.

Podrá:

- Activar o desactivar la cámara en cualquier momento.
- Elegir entre distintos niveles de descripción (por ejemplo, omitir rostros o detalles de personas).
- Activar un modo de privacidad reforzada, que elimina cualquier registro o configuración tras su uso.

El sistema informará, al iniciar su uso, de forma transparente y accesible, mediante mensajes de voz o texto, sobre qué datos se procesan, cómo y con qué finalidad.

1.4. Riesgos de privacidad identificados

1. Grabación involuntaria de terceros: personas que no han dado su consentimiento pueden ser captadas por la cámara.
2. Tratamiento de datos sensibles: rasgos faciales o comportamientos pueden ser procesados de forma inadvertida.
3. Fuga de información si el dispositivo fuera hackeado.
4. Errores de la IA o sesgos en la descripción (por ejemplo, interpretaciones subjetivas o discriminatorias).

5. Dependencia tecnológica: el usuario podría confiar ciegamente en la IA, reduciendo su atención al entorno real.

1.5. Estrategias de mitigación

1. Privacidad por diseño → todos los datos se procesan en local sin almacenarse.
2. Mecanismo de detección de zonas sensibles → pausa automática del procesamiento visual.
3. Política de retención nula → no se guarda ningún dato personal tras finalizar el uso.
4. Pruebas de sesgo e imparcialidad → validación previa con diferentes entornos culturales y demográficos.
5. Formación al usuario → programa de adaptación que fomente la complementariedad con el bastón y la escucha activa.

2. Mapa de datos y principio de minimización

Tipo de dato	Origen	Finalidad	Base legal (GDPR)	Retención	Medida de minimización
Imagen de vídeo	Cámara de las gafas	Descripción del entorno	Art. 9.2.g – accesibilidad Interés legítimo	No se almacena	Procesamiento local + borrado inmediato
Datos de configuración	Usuario	Personalización de uso	Ejecución de contrato	Mientras dure el uso	Datos no personales, cifrados localmente
Telemetría técnica	Sistema	Mejora de rendimiento	Interés legítimo	2 semanas	Sin datos personales identificables

Explicación de las Bases legales:

Imagen de vídeo del entorno (art. 6 RGPD):

- Interés legítimo (art. 6.1.f) → si el tratamiento es necesario para el funcionamiento del sistema y no vulnera derechos de terceros.
- Tratamiento de datos especiales (datos biométricos)

Datos de configuración:

- Ejecución de contrato (art. 6.1.b) → necesarios para prestar el servicio.

Telemetría técnica:

- Interés legítimo (art. 6.1.f) → mantenimiento, seguridad y mejora del sistema.

3. Clasificación según IA Act y cumplimiento GDPR/LOPDGDD

Aspecto	Evaluación / Clasificación
Nivel de riesgo IA Act	Alto riesgo (anexo III – accesibilidad y datos biométricos)
Requisitos IA Act	Evaluación técnica, registro en base europea
Base jurídica GDPR	Interés legítimo (art. 6.1.f) + finalidad de accesibilidad (art. 9.2.g)
Principios aplicables	Minimización, limitación de finalidad, privacidad por diseño
Derechos de los interesados	Acceso, rectificación, oposición, eliminación
Responsable del tratamiento	Empresa desarrolladora del sistema
Medidas técnicas	Procesamiento local, cifrado, borrado inmediato
Supervisión humana	Usuario mantiene control total sobre el dispositivo

4. Retención y borrado (política y procedimiento de purga)

El objetivo es garantizar que todos los datos personales captados por las gafas inteligentes de CegadosPorLaIA sean tratados de forma temporal, segura y respetando la privacidad de usuarios y terceros, cumpliendo con GDPR y LOPDGDD.

Política de retención de datos:

1. Procesamiento local y temporal:

- Todas las imágenes captadas se procesan exclusivamente en el dispositivo, sin almacenamiento permanente.
- No se transfieren datos personales a servidores externos ni a terceros.

2. Datos de configuración y telemetría:

- La información de configuración del usuario se mantiene solo durante la sesión activa y se elimina al finalizar el uso.
- La telemetría técnica (información no personal sobre funcionamiento del sistema) se retiene un máximo de 2 semanas, únicamente para mejorar rendimiento y detectar fallos, sin contener información personal identificable.

Procedimiento de purga:

1. Al finalizar cada sesión, el sistema ejecuta un borrado automático de:
 - Imágenes de vídeo.
 - Datos de configuración temporal.
2. En caso de reinicio, apagado o fallo del dispositivo, los datos residuales son eliminados automáticamente al reiniciar el sistema.
3. Los usuarios pueden activar un modo de privacidad reforzada, que asegura la eliminación inmediata de cualquier dato almacenado temporalmente durante la sesión.

Uso de IA:

- Apartado 1.2: [Bases legales](#)
- Apartado 2: [Bases legales](#)