IA ciudadana

Nota de posición: AI Ómnibus | 16 de junio de 2026

El Parlamento Europeo ha aprobado el denominado *AI Ómnibus*, un paquete presentado como simplificación del Reglamento de Inteligencia Artificial (AI Act) que, en la práctica, debilita garantías antes de que estas hayan llegado a aplicarse. IA Ciudadana analiza cuatro aspectos clave de este acuerdo que afectan a la transparencia, a los derechos fundamentales, a la participación ciudadana y a la gobernanza democrática de la IA.

1. Registro europeo de sistemas de IA (Art. 6.3): menos información pública, menos control ciudadano

La propuesta inicial de la Comisión planteaba eliminar completamente la obligación de registro público para proveedores que, amparándose en el artículo 6(3) del AI Act, deciden de forma unilateral que su sistema no debe clasificarse como de alto riesgo. Esta propuesta no prosperó en el trílogo, lo que es positivo.

Sin embargo, el texto final sí reduce la información que debe publicarse en la base de datos europea: desaparecen, entre otros datos, los Estados miembros donde el sistema se comercializa y los motivos concretos por los que el proveedor considera que su sistema no es de alto riesgo.

Nuestra valoración: El registro europeo es una de las pocas herramientas que permite a la ciudadanía, a la sociedad civil y a los investigadores saber qué sistemas de IA están desplegándose, dónde y con qué justificaciones. Sin esa información, la auto-exención del artículo 6(3) queda sin control público efectivo. Un proveedor puede decidir que su sistema —aunque opere en ámbitos como el empleo, la educación o el los servicios sociales— no es de alto riesgo, y nadie podrá verificarlo fácilmente. Desde IA ciudadana consideramos que esta reducción de transparencia debilita la rendición de cuentas y dificulta cualquier forma de supervisión ciudadana independiente.

2. Retrasos en las obligaciones para IA de alto riesgo: más tiempo sin garantías

El acuerdo pospone el cumplimiento de las obligaciones para sistemas de alto riesgo del Anexo III (que incluye IA usada en empleo, educación, servicios esenciales, migración y justicia) hasta el 2 de diciembre de 2027. Para sistemas del Anexo I (que incluye las prácticas y sistemas prohibidos), el plazo se extiende al 2 de agosto de 2028. Las autoridades públicas y los sistemas desplegados en su nombre no estarán sujetos a las obligaciones hasta el 2 de agosto de 2030.

Nuestra valoración: Este aplazamiento no es una decisión técnica neutral: es una decisión política que prolonga el período en que personas en situaciones vulnerables —usuarias de servicios públicos, personas dentro del sistema de justicia, solicitantes de prestaciones sociales, pacientes— quedan expuestas a sistemas de IA sin las garantías que la propia AI Act establecía como necesarias.

El retraso hasta 2030 para las autoridades públicas es especialmente preocupante. Las administraciones públicas son, con frecuencia, los actores que más directamente despliegan IA en contextos que afectan a derechos: asignación de ayudas, valoración de riesgos, toma de decisiones en servicios sociales. Posponer la aplicación de salvaguardas en este ámbito retrasa también el acceso ciudadano a mecanismos de impugnación y revisión humana.

Además, el retraso crea un incentivo perverso: los proveedores pueden acelerar el despliegue de sistemas antes del nuevo plazo, anticipando tecnologías que quizás no estén listas para cumplir. Las preocupaciones sobre guías de implementación y preparación debían haberse abordado con más recursos para las autoridades de supervisión, no reabriendo la ley.

---

3. Evaluaciones de Impacto en Derechos Fundamentales (FRIA - por sus siglas en inglés): preservadas, pero en riesgo de vaciarse

Las FRIA o EIDF —la obligación para los desplegadores de sistemas de IA de alto riesgo de evaluar el impacto sobre los derechos fundamentales— se han preservado en el texto final, lo que valoramos positivamente como resultado de la presión sostenida de la sociedad civil.

Sin embargo, el texto final permite hacer referencia cruzada a las Evaluaciones de Impacto en Protección de Datos (DPIA cuando estas cubran los mismos elementos requeridos por el artículo 27 del AI Act.

Nuestra valoración: Las FRIAs y las DPIA no son equivalentes. Una DPIA se centra en los riesgos asociados al tratamiento de datos personales; en la práctica, la mayoría se limita a aspectos de seguridad de los datos. Una FRIA debe ir más lejos: analizar el contexto institucional de despliegue, el acceso a servicios, los desequilibrios de poder, las condiciones laborales, la participación de los grupos potencialmente afectados antes del despliegue del sistema, la capacidad de las personas afectadas para impugnar decisiones automatizadas, y los impactos sobre grupos específicos en situación de vulnerabilidad.

Desde IA Ciudadana, las FRIA son también una oportunidad para incorporar procesos de participación de las comunidades afectadas en la evaluación de los sistemas de IA. Esto es central para una gobernanza democrática de la IA.

El riesgo es que, en la práctica, muchas organizaciones utilicen la referencia cruzada para evitar hacer una FRIA real, asumiendo que la DPIA ya cubre todo. La plantilla que elabore la Oficina de IA de la UE y la guía de implementación serán determinantes para que las FRIA sigan siendo herramientas reales de responsabilidad, y no un trámite vacío.

4. Artículo 77: acceso indirecto para los organismos de derechos fundamentales

El texto final mantiene un modelo de acceso indirecto para los organismos de derechos fundamentales —instituciones de igualdad, defensores del pueblo, organismos de supervisión sectorial—: podrán acceder a información y documentación sobre sistemas de IA a través de las autoridades de vigilancia del mercado, pero no directamente bajo el

propio AI Act. Un recital aclara que los poderes existentes bajo otra normativa no quedan limitados, pero esto no resuelve el problema estructural.

Nuestra valoración: Este modelo de intermediación debilita la supervisión independiente precisamente en los contextos más sensibles: sistemas de IA utilizados por fuerzas de seguridad, administraciones de extranjería, o sistemas automatizados de asignación de recursos públicos. Son exactamente los ámbitos donde los organismos especializados en derechos fundamentales tienen la experiencia, el mandato y la legitimidad para supervisar directamente.

Añadir intermediación burocrática ralentiza el acceso a la información y puede dejar sin respuesta situaciones urgentes de vulneración de derechos. Desde IA ciudadana entendemos que la supervisión efectiva de la IA en manos del Estado es una condición básica de la democracia: sin acceso directo de organismos independientes a los sistemas que pueden afectar derechos, la rendición de cuentas se convierte en un proceso opaco y lento.

Conclusión

El AI Omnibus recién aprobado debilita las herramientas con las que la ciudadanía y sus organizaciones pueden exigir rendición de cuentas a los sistemas de IA que les afectan. Reduce la información pública disponible sobre sistemas auto-exentos, pospone garantías en sectores críticos, abre la puerta a que las FRIA se vacíen de contenido, y complica la supervisión independiente en el ámbito de los derechos fundamentales.

Desde IA ciudadana reclamamos:

- Que la implementación del registro europeo recupere, como mínimo, los elementos de transparencia eliminados por el Ómnibus.
- Que la Oficina de IA de la UE desarrolle guías de implementación que garanticen que las FRIA incluyen procesos participativos con las comunidades afectadas y no se reducen a una referencia cruzada con la DPIA.
- Que los Estados miembros doten de recursos suficientes a las autoridades de supervisión para que puedan aplicar las obligaciones del AI Act sin necesidad de nuevos aplazamientos.
- Que se rechace el modelo Ómnibus como vía para reabrir salvaguardas de derechos digitales antes de que estas hayan tenido oportunidad de aplicarse.

Esta nota se basa en el análisis conjunto de EDRi, Access Now, AlgorithmWatch, Amnesty International y otros miembros de la red EDRi: AI Omnibus: a rollback of AI safeguards before they even apply (junio de 2026).