

ENFOQUE CORPORATIVO

Procesamiento de datos sensibles en sistemas IA



**Daniela
Chávez**

Asociada del área
de protección
de datos-Estudio
Olachea

El pasado 10 de setiembre venció el primer plazo de adecuación del Reglamento de la Ley N.º 31814, Ley que promueve el uso de la inteligencia artificial (IA), aprobado mediante Decreto Supremo N.º 115-2025-PCM. Desde esa fecha, los desarrolladores e implementadores de sistemas de IA en los sectores de salud, educación, justicia, seguridad, economía y finanzas deben cumplir con obligaciones de transparencia algorítmica, supervisión humana, políticas internas y registro documentado de los sistemas de IA clasificados como sistemas de riesgo alto.

Al respecto, no es casualidad que el legislador priorizara justamente estos seis sectores, dado que son los que potencialmente pueden tratar grandes volúmenes de datos personales clasificados como sensibles bajo la Ley de Protección de Datos Personales, Ley N.º 29733 (LPDP), y su reglamento, Decreto Supremo N.º 016-2024-JUS. La LPDP califica como sensibles los datos biométricos, de salud, ingresos económicos, afiliación sindical, entre otros. El propio reglamento de la Ley de la IA lo reconoce y remite a la LPDP, precisando que las sanciones por el mal uso de los datos se rigen por la LPDP y su reglamento, cuyas multas pueden oscilar desde 0.5 hasta 100 UIT; y, para el caso concreto de datos sensibles, entre las 5 y 100 UIT.

Producto de ello, en la práctica, un sistema que oriente diagnósticos o priorice pacientes usando historias clínicas electrónicas, o uno que evalúe

el riesgo crediticio de una persona clasifica como sistemas de riesgo alto, precisamente por procesar datos sensibles con capacidad de generar impactos significativos en los derechos y libertades de los individuos. Además, está expresamente prohibido utilizar datos biométricos para inferir origen étnico, opiniones políticas o vida sexual.

Entonces, ¿cómo podemos garantizar que estas entidades alimenten sus sistemas de IA con datos sensibles sin infringir la LPDP? El punto de partida es identificar la base legal del tratamiento de los datos para evaluar la licitud de la base de datos, sumado a la implementación de la privacidad desde el diseño: minimizar los datos recolectados, anonimizar o seudonimizar cuando sea posible, y documentar las finalidades del algoritmo y las fuentes usadas.

Asimismo, se recomienda hacer una evaluación de impacto de protección de datos personales y articular al Oficial de Datos Personales al momento de habilitar sistemas de IA en las entidades. Por lo tanto, aunque todavía se encuentran pendientes ciertos lineamientos específicos para la implementación de sistemas de IA, ello no suspende las obligaciones que ya resultan exigibles. En este contexto, la LPDP y su Reglamento constituyen el punto de partida para determinar si el tratamiento resulta lícito y qué salvaguardas deben implementarse, sin perjuicio de las obligaciones adicionales que correspondan por la naturaleza y nivel de riesgo del sistema de IA. Así, el cumplimiento no debería abordarse como una etapa posterior al desarrollo del sistema, sino como un componente integral de su diseño, implementación y supervisión.