https://doi.org/10.18800/dys.202601.006

FECHA DE RECEPCIÓN: 20/11/2025
FECHA DE APROBACIÓN: 16/03/2026

La inteligencia artificial en el Perú: análisis normativo en torno al ciclo de vida del dato personal y de los sistemas de IA

Artificial intelligence in Peru: a regulatory analysis of the personal data and AI systems lifecycles

Alexandra Espinoza Montero*
Benites, Vargas & Ugaz Abogados

Resumen:
El presente artículo analiza, mediante un enfoque de análisis normativo comparado, la interrelación entre el ciclo de vida de los sistemas de inteligencia artificial (IA) y el ciclo de vida de los datos personales, con énfasis en las obligaciones de privacidad y protección de datos que emergen en cada etapa. Para ello, se integran normas internacionales —como el Reglamento de Inteligencia Artificial de la Unión Europea, el Reglamento General de Protección de Datos (RGPD), las guías de la OCDE y las normas ISO— junto con el marco normativo peruano, destacando la importancia de adoptar medidas que permitan identificar riesgos en cada etapa.
Asimismo, se examinan los roles de los distintos agentes involucrados —proveedor, responsable del despliegue, importador, representante autorizado, distribuidor y encargado del tratamiento— a fin de delimitar responsabilidades específicas en torno al tratamiento de datos personales. El artículo enfatiza la necesidad de aplicar los principios de *privacy by design* y *privacy by default*, así como evaluaciones de impacto y auditorías algorítmicas para prevenir riesgos como la discriminación, el sesgo o la falta de transparencia. Finalmente, se formulan recomendaciones orientadas a fortalecer un marco regulatorio nacional que sea coherente con los estándares internacionales, concluyendo que una aproximación regulatoria flexible, basada en principios y complementada con instrumentos técnicos como normas ISO, resulta más eficaz que una regulación rígida para promover una implementación responsable y ética de la IA en el Perú, preservando al mismo tiempo los derechos fundamentales de las personas.

Abstract:
This article examines, through a comparative regulatory analysis, the relationship between the lifecycle of artificial intelligence (AI) systems and the lifecycle of personal data, with a particular focus on privacy and data protection obligations arising at each stage. Using a

* Abogada asociada del área de Competencia y Propiedad Intelectual del estudio Benites, Vargas & Ugaz Abogados. Cuenta con amplia experiencia en temas relacionados a la propiedad intelectual, protección de datos personales, derecho del consumidor, derecho de la competencia y derecho administrativo en general.
Destaca por sus conocimientos en Derecho y Nuevas Tecnologías (IT). Obtuvo su título como abogada con la sustentación de su tesis sobre Derechos de Autor en Internet, aprobada con la mención de Sobresaliente (*summa cum laude*). Ha escrito diversos artículos sobre propiedad intelectual y protección de datos en portales jurídicos, revistas académicas y periódicos nacionales. Además, es autora del libro "Anarquía virtual: Derechos de autor en Internet y regulación en la era de las plataformas de streaming" publicado con Palestra Editores.

comparative perspective, it integrates international standards —such as the European Union Artificial Intelligence Act, the General Data Protection Regulation (GDPR), OECD guidelines, and ISO standards— with the Peruvian regulatory framework, stressing the importance of implementing safeguards that allow identifying risks in each stage.
The roles of the main actors —provider, deployer, importer, authorized representative, distributor, and processor— are analyzed to clarify specific responsibilities regarding personal data processing. The article highlights the need to apply the principles of *privacy by design* and *privacy by default*, as well as impact assessments and algorithmic audits, to prevent risks such as discrimination, bias, and lack of transparency. Finally, it puts forward recommendations to strengthen the national regulatory framework in alignment with international standards, concluding that a flexible, principle-based regulatory approach, complemented by technical instruments such as ISO standards, is more effective than rigid regulation in fostering responsible and ethical AI implementation in Peru while safeguarding fundamental rights.

Palabras clave:
Inteligencia artificial – Protección de datos personales – Privacidad desde el diseño – Ciclo de vida de la IA – Evaluación de impacto.

Keywords:
Artificial intelligence – Personal data protection – Privacy by design – AI lifecycle – Impact assessment.

1. Introducción

La inteligencia artificial (en adelante, IA) plantea interrogantes trascendentes sobre cómo debe aplicarse y adaptarse la regulación para evitar que su desarrollo y uso afecten derechos fundamentales. La IA puede contribuir al crecimiento económico y al bienestar social de las personas; sin embargo, es indispensable entender la problemática que puede surgir con su implementación, tal como la potencial violación de derechos fundamentales (Sánchez, 2022).

Por un lado, un sector exige que la IA se expanda y permita que evolucione con total libertad, priorizando su innovación. Por otro lado, se enfatiza que este crecimiento no puede ser descontrolado. En consecuencia, resulta necesario establecer pautas que garanticen la protección de los derechos y libertades individuales de las personas que pueden verse afectadas por el desarrollo y uso de sistemas de IA (Iturmendi, 2024).

El mercado de la IA ha crecido de forma acelerada. Se estima que, para el año 2027, su valor superará los 400 000 millones de dólares estadounidenses (Statista, 2025). Este crecimiento exponencial ha motivado la creación de principios rectores y directrices que orienten cómo debe diseñarse, desarrollarse y utilizarse la IA, con el propósito de asegurar su "ética" y "fiabilidad". Ello ha derivado en la conformación de grupos de expertos, así como en iniciativas impulsadas por instituciones académicas y organismos internacionales que han trabajado activamente en propuestas para gobernar la IA de manera responsable. Todas estas acciones buscan establecer reglas que permitan gestionar los riesgos y aprovechar las oportunidades asociados con la IA (Organización para la Cooperación y el Desarrollo Económicos [OCDE], s. f.).

Estas iniciativas no solo persiguen la construcción de bases éticas, sino que también sirven como insumos para la creación de Códigos de Conducta y marcos normativos vinculantes. Diversos países —incluido el Perú— han suscrito documentos internacionales sobre IA o han adoptado normativa inspirada en tales instrumentos.

Uno de los aspectos más discutidos y desarrollados en cada uno de estos documentos es la gestión de la privacidad y la protección de datos personales, esta última concebida como una concreción normativa del derecho a la intimidad. Dicha preocupación responde a que los sistemas de IA suelen "alimentarse" de grandes volúmenes de información personal y sensible, cuyo tratamiento inadecuado puede derivar en prácticas discriminatorias, sesgos algorítmicos, usos indebidos de datos recopilados en Internet o violaciones al principio de consentimiento informado, entre otros. Por este motivo, la privacidad y la protección de datos se han convertido en ejes transversales en las agendas regulatorias internacionales y nacionales, en tanto constituyen la base para garantizar la confianza pública en el uso de la IA.

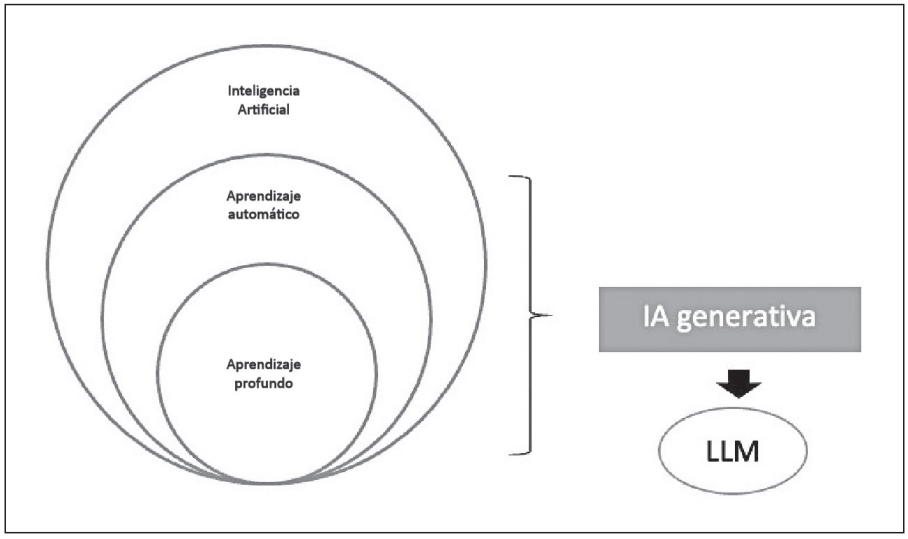
El presente artículo tiene como objetivo analizar el impacto que el desarrollo y uso de sistemas de IA genera sobre la privacidad y la protección de

datos personales en el Perú. Para ello, se considera que es indispensable correlacionar el ciclo de vida del sistema de IA con el ciclo de vida de los datos personales para identificar y examinar los riesgos asociados al tratamiento de información, conforme a la normativa vigente tanto nacional como internacional. Asimismo, se evaluarán las respuestas normativas nacionales actualmente en vigor, las propuestas legislativas en curso y, de manera complementaria, las principales iniciativas regulatorias internacionales, con especial énfasis en la necesidad de enfoques regulatorios que garanticen la protección efectiva de los derechos fundamentales sin obstaculizar el avance tecnológico. Finalmente, el análisis se complementará con recomendaciones aplicables a cada etapa del ciclo de vida de la IA, en correlato con el ciclo de vida de los datos personales, con el propósito de contribuir al diseño de un marco regulatorio equilibrado que promueva la innovación responsable y el respeto por la privacidad y la protección de datos personales.

2. Definiciones importantes

Para abordar de manera rigurosa el análisis propuesto, resulta imprescindible delimitar y precisar los conceptos clave que serán empleados a lo largo del presente artículo. En consecuencia, este primer apartado tiene como finalidad compilar, comparar y delimitar las definiciones existentes sobre IA, sistemas de IA, aprendizaje automático (*machine learning*), aprendizaje profundo (*deep learning*) e IA generativa (en adelante, IAGen). El establecimiento de un marco conceptual claro y actualizado facilitará la comprensión integral de los temas que se desarrollarán en las secciones posteriores.

Gráfico 1. Conceptos importantes sobre IA



Fuente: Elaboración propia a partir de Irazabal (2024), UNESCO (2021) y OCDE (s. f.).

La definición de estos términos se fundamentará en una revisión de la normativa internacional y nacional vigente, incluyendo tanto leyes como reglamentos aplicables. Asimismo, se incorporarán guías, directrices y políticas elaboradas por organismos internacionales de referencia, tales como la Organización para la Cooperación y el Desarrollo Económico (en adelante, OCDE), la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (en adelante, UNESCO) y la Unión Europea (en adelante, UE), que han contribuido significativamente a la estandarización conceptual en la materia.

Finalmente, se considerarán los proyectos de ley actualmente en discusión en el ámbito nacional, así como doctrina relevante, con el objetivo de identificar tendencias regulatorias emergentes y posibles modificaciones futuras en la definición de estos conceptos. El análisis comparativo e integral de estos elementos permitirá identificar el estado actual y las perspectivas de evolución de las definiciones oficiales, así como sus implicancias para la protección de datos personales y la privacidad.

a. Inteligencia artificial (IA)

La primera regulación que existió sobre IA, debidamente desarrollada y de aplicación general, fue el Reglamento 2024/1689, Reglamento de Inteligencia Artificial de la Unión Europea (en adelante, RIA). Dicho reglamento se elaboró en un contexto en el que no existía consenso doctrinal ni científico acerca de una definición precisa de IA, lo que representó un desafío adicional dada la rápida evolución tecnológica, capaz de volver obsoletas las definiciones en un corto plazo (Blanes, 2025).

Según Blanes (2025), la IA presenta dos características esenciales: la **autonomía**, entendida como la capacidad de ejecutar tareas complejas sin la intervención directa del usuario, y la **adaptabilidad**, es decir, la facultad de aprender a partir de la experiencia. A ello se añade un tercer elemento inherente: la **generación de respuestas**. En esa línea, la aproximación de la UE fue adoptar una definición "humanista" de la IA, centrada en una perspectiva cercana al ciudadano (Blanes, 2025).

Por este motivo, la Comisión Europea, en el documento denominado "Comunicación al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones (2018)", definió a la IA como "sistemas que manifiestan un comportamiento inteligente, pues son capaces de analizar su entorno y pasar a la acción —con cierto grado de autonomía— con el fin de alcanzar objetivos específicos" (p. 1)[1]. Esta definición fue desarrollada por el mismo Grupo Independiente de Expertos de Alto Nivel sobre IA en el documento denominado "Una definición de la inteligencia artificial: principales capacidades y disciplinas científicas" en el 2019.

En el documento, el Grupo de Expertos (2019) define a la IA como una disciplina científica, de la siguiente forma:

> La IA es una disciplina científica que incluye varios enfoques y técnicas, como el aprendizaje automático (del que el aprendizaje profundo y el aprendizaje por refuerzo constituyen algunos ejemplos), el razonamiento automático (que incluye la planificación, programación, representación y razonamiento de conocimientos, búsqueda y optimización) y la robótica (que incluye el control, la percepción, sensores y accionadores así como la integración de todas las demás técnicas en sistemas ciberfísicos) (p. 6).

Por su parte, la OCDE (2019) define a la IA como "un conjunto de tecnologías que combinan datos, algoritmos y potencia de cómputo para realizar tareas que normalmente requieren inteligencia humana". La OCDE ha sido una de las organizaciones internacionales que se ha preocupado por la elaboración de documentos que permitan uniformizar recomendaciones y conceptos en el desarrollo de la IA. La OCDE (s. f.) dispone que, con el fin de que los gobiernos colaboren en la gestión de la IA a nivel internacional, es necesario utilizar términos y definiciones comunes que sirvan como base para la cooperación.

El Decreto Supremo N.° 041-2023-PCM declara de interés nacional el proceso de adhesión del Perú a la OCDE, por lo que es relevante considerar los conceptos propuestos por dicha organización con el fin de que sean incorporados en nuestra regulación.

En el contexto peruano, el concepto de IA se encuentra descrito en la Ley N.° 31814, Ley que promueve el uso de la Inteligencia Artificial en favor del desarrollo económico y social del país (en adelante, Ley de IA). El literal a) del artículo 3 de la Ley de IA la define como una "tecnología emergente de propósito general que tiene el potencial de mejorar el bienestar de las personas, contribuir a una actividad económica global sostenible positiva, aumentar la innovación y la productividad, y ayudar a responder a los desafíos globales clave".

De manera complementaria, la Presidencia del Consejo de Ministros (en adelante, PCM) habilitó un portal web en la plataforma digital del Estado Peruano, en el que describe el abordaje nacional de la IA[2] y la define como "un campo de la informática que se dedica a crear sistemas capaces de tomar decisiones o realizar tareas de manera similar a la inteligencia humana" (Presidencia del Consejo de Ministros [PCM], 2021). Recientemente, la PCM (2025) publicó el Decreto Supremo N.° 115-2025-PCM, Reglamento de la Ley de IA (en adelante, Reglamento de la Ley de IA), el cual complementa la definición de la IA de la siguiente forma:

> i. IA: Disciplina científica orientada a la investigación y desarrollo de sistemas basados en IA.

Por último, existen diversos proyectos de ley que, a la fecha, se encuentran siendo discutidos en las comisiones del congreso respectivas, las cuales proponen diversas definiciones de la IA. A continuación, mostramos algunos de los más importantes:

1 El detalle se encuentra en el documento identificado con número "Bruselas, 25.4.2018 COM(2018) 237 final".
2 Se puede acceder a la plataforma en el siguiente enlace: https://www.gob.pe/es/institucion/pcm/tema/19283-inteligencia-artificial

P.L 5183/2022 que fomenta uso de IA para mejora de seguridad ciudadana[3]	P.L 7033/2023-CR Ley que regula el desarrollo del uso de la Inteligencia Artificial en el Perú[4]	P.L 8223/2023-CR, Proyecto de Ley de fomento y regulación del uso de la inteligencia artificial en el Perú[5]	P.L. 8969/2024-CR, Proyecto de Ley que promueve el uso de la inteligencia artificial en el sistema financiero del país[6]
"Conjunto de técnicas, algoritmos, herramientas y metodologías que permiten a las máquinas imitar y superar el desempeño humano en tareas específicas"	*"La combinación de algoritmos planteados con el propósito de crear máquinas que presenten las mismas capacidades que el ser humano"*	*"Conjunto de técnicas y tecnologías que permiten a las máquinas realizar tareas que requieren inteligencia humana"*	*"Campo de la informática que se enfoca en crear sistemas que pueden realizar tareas que normalmente requieren inteligencia humana, como el aprendizaje, el razonamiento y la percepción"*

Fuente: Elaboración propia.

Las definiciones de IA recogidas en este apartado comparten elementos en común: la autonomía de los sistemas, la adaptabilidad mediante el aprendizaje a partir de datos o experiencias, y la capacidad de generar respuestas o tomar decisiones orientadas al cumplimiento de objetivos. Asimismo, la mayoría de las definiciones enfatiza el uso de algoritmos y modelos computacionales avanzados, así como la integración de diversas disciplinas, entre ellas el aprendizaje automático, el razonamiento lógico y la robótica.

Considerando el entorno peruano, es fundamental uniformizar la definición de IA, pues la coexistencia de múltiples conceptos en distintos cuerpos normativos puede generar ambigüedades y dificultades interpretativas que afectan la seguridad jurídica y la aplicación coherente de las normas. Una definición clara y alineada con los estándares internacionales permitiría integrar la regulación nacional en el marco global.

Finalmente, cabe destacar que los sistemas informáticos pueden incorporar o utilizar IA como parte de su funcionamiento, lo que permite diferenciar entre sistemas convencionales y sistemas basados en IA.

b. Sistemas basados en la IA

El concepto de "sistema de IA" o "sistema basado en la IA" es uno de los más desarrollados y discutidos a nivel internacional y nacional. Existen diversas fuentes que delimitan su significado, por lo que en el presente apartado nos centraremos en algunas de las definiciones más relevantes.

El Grupo Independiente de Expertos creado por la Comisión Europea (2019) definió a los sistemas de IA de la siguiente forma:

> Los sistemas de inteligencia artificial (IA) son sistemas de software (y en algunos casos también de hardware) diseñados por seres humanos que, dado un objetivo complejo, actúan en la dimensión física o digital mediante la percepción de su entorno a través de la obtención de datos, la interpretación de los datos estructurados o no estructurados que recopilan, el razonamiento sobre el conocimiento o el procesamiento de la información derivados de esos datos, y decidiendo la acción o acciones óptimas que deben llevar a cabo para lograr el objetivo establecido. Los sistemas de IA pueden utilizar normas simbólicas o aprender un modelo numérico; también pueden adaptar su conducta mediante el análisis del modo en que el entorno se ve afectado por sus acciones anteriores (p. 6).

Esta definición guarda similitud con la contenida en el RIA, que entiende por sistema de IA a:

> un sistema basado en una máquina que está diseñado para funcionar con distintos niveles de autonomía y que puede mostrar capacidad de adaptación tras el despliegue, y que, para objetivos explícitos o implícitos, infiere de la información de entrada que recibe la manera de generar resultados de salida, como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos físicos o virtuales

3 Al 10 de agosto de 2025, el proyecto de ley se encuentra en comisión.
4 Al 10 de agosto de 2025, el proyecto de ley se encuentra en comisión y se ha emitido un dictamen de inhibición por parte de la Comisión de Presupuesto y Cuenta General de la República. Deberá ser discutido únicamente en la Comisión de Ciencia, Innovación y Tecnología.
5 Al 10 de agosto de 2025, el proyecto de ley se encuentra en comisión.
6 Al 10 de agosto de 2025, el proyecto de ley se encuentra en comisión.

Por su parte, la OCDE (2019) define a los sistemas de IA de forma similar a lo dispuesto en el RIA:

> Sistema de IA: Un sistema de IA es un sistema basado en máquinas que, para objetivos explícitos o implícitos, infiere, a partir de los datos de entrada que recibe, cómo generar información de salida como predicciones, contenidos, recomendaciones o decisiones, que pueden influir en entornos reales o virtuales. Una vez implementados, los distintos sistemas de IA presentan diversos niveles de autonomía y varían en su capacidad de adaptación.

La UNESCO (2021) los define como un "sistema basado en la máquina que puede hacer predicciones, recomendaciones o tomar decisiones, influyendo en entornos reales o virtuales, sobre ciertos objetivos definidos por los humanos".

En atención al manual de Russel y Norvig, citado por el Grupo de Expertos (2019) en su documento de trabajo sobre la definición de IA, un sistema de IA se caracteriza por ser racional. Esta racionalidad es alcanzada

> percibiendo el entorno en el que se encuentra inmerso el sistema a través de sensores, recopilando e interpretando datos, razonando sobre lo que percibe o procesando la información derivada de esos datos, decidiendo cuál es la mejor acción que puede realizar y actuando en consecuencia mediante accionadores, pudiendo así modificar el entorno (Grupo de Expertos, 2019, p. 1).

En el contexto peruano, la Ley de IA propone una definición para *los "sistemas basados en inteligencia artificial".* De esta forma, se entiende por sistema basado en IA a aquel "sistema electrónico-mecánico que puede, para una serie de objetivos definidos por humanos, hacer predicciones, recomendaciones o tomar decisiones, influenciando ambientes reales o virtuales. Está diseñado para funcionar con diferentes niveles de autonomía".

El Reglamento de la Ley de IA (PCM, 2025) reitera esta definición y la desarrolla de forma complementaria de la siguiente forma:

> j. Sistema basado en IA: Sistema basado en máquina que, para objetivos de forma explícita o implícita, infiere, a partir de la entrada que recibe, cómo generar salidas tales como predicciones, contenido, recomendaciones o toma de decisiones que puedan influir en la o los entornos físicos o digitales. Los diferentes sistemas basados en IA varían en sus niveles de autonomía y la capacidad de entendimiento y adaptación después del despliegue.

Además, algunos proyectos de ley recientes han introducido nociones específicas. Por ejemplo, el Proyecto de Ley N.° 7033/2023-CR define al "sistema de inteligencia artificial autónomo (SIAA)" como "un sistema de IA capaz de operar de manera independiente sin intervención humana directa". Por su parte, el Proyecto de Ley N.° 8223/2023-CR describe al sistema de IA como "el conjunto de algoritmos, datos y procesos que permiten la operación de un sistema de inteligencia artificial".

En síntesis, las distintas definiciones revisadas coinciden en señalar que los sistemas de IA son estructuras basadas principalmente en *software* —y, en algunos casos también en *hardware*—, diseñadas por seres humanos para cumplir objetivos determinados, operando en entornos físicos o digitales mediante la percepción, interpretación y procesamiento de datos. Estos sistemas son capaces de generar predicciones, recomendaciones, decisiones o contenidos que inciden en dichos entornos. Asimismo, comparten tres características esenciales:

- Autonomía, entendida como la capacidad de operar con distintos niveles de independencia respecto de la intervención humana.
- Adaptabilidad, que supone la posibilidad de aprender y modificar su comportamiento en función de la experiencia y de los resultados obtenidos.
- Racionalidad, expresada en la toma de decisiones orientadas al logro de objetivos específicos

c. *Machine learning* o aprendizaje automático

El aprendizaje automático, conocido internacionalmente como *machine learning*, constituye una de las subdisciplinas fundamentales de la IA. De acuerdo con la definición clásica propuesta por Tom Mitchell, citada por el Centro Nacional de Planeamiento Estratégico (en adelante, CEPLAN), el *machine learning* es "un programa computacional que aprende a realizar la tarea T y obtiene mejores resultados en la medida P a través de la experiencia" (Centro Nacional de Planeamiento Estratégico [CEPLAN], 2021, p. 17). En términos generales, puede describirse como un conjunto de modelos y técnicas que permiten a los sistemas informáticos aprender de manera autónoma a partir de datos, identificando patrones sin necesidad de ser programados explícitamente para cada tarea específica.

El RIA hace referencia al aprendizaje automático como uno de los antecedentes y técnicas que sustentan la construcción de sistemas de IA. En el considerando 12 de la norma, se describe que el *machine learning* posibilita que la IA aprenda de los datos cómo alcanzar objetivos y estrategias, basándose en la lógica y el conocimiento inferido a partir de representaciones simbólicas de las tareas a

resolver (Parlamento Europeo y Consejo de la Unión Europea, 2024).

De forma complementaria, la OCDE (2019) define al *machine learning* como la capacidad de los sistemas para "ajustar su comportamiento de forma autónoma basándose en experiencias previas". En la misma línea, la Comisión Europea (2021) lo describe como "el campo de estudio que da a las computadoras la capacidad de aprender sin ser explícitamente programadas". Por su parte, la UNESCO (2021) resalta que esta técnica permite a los sistemas identificar patrones complejos en grandes volúmenes de datos y utilizarlos para tomar decisiones o realizar predicciones.

Desde la doctrina, Blanes (2025) entiende al *machine learning* como una rama de la IA que programa algoritmos para que aprendan por sí mismos y generen resultados sin intervención humana directa. De acuerdo con este autor, se trata de una técnica que "no depende exclusivamente de lo que el humano le ha proporcionado anteriormente, sino que permite que sea el propio sistema quien determine la forma de abordar la solución" (2025, p. 40).

En el contexto peruano, conforme a lo dispuesto en la Plataforma del Estado Peruano en la que se desarrollan diversos conceptos relacionados con la IA, se describe que el *machine learning* es un "método de aprendizaje en el que se le brindan patrones de datos repetidos de diferentes maneras para que la IA pueda identificarlos en otros contextos" (PCM, s. f.).

En conclusión, el *machine learning* puede entenderse como el conjunto de algoritmos, modelos y técnicas que permiten a las máquinas aprender automáticamente a partir de datos, detectar patrones e inferir soluciones sin seguir instrucciones rígidas previamente programadas por los humanos. Esta capacidad es esencial para que los sistemas de IA mejoren su rendimiento con el tiempo, se adapten a nuevos contextos y evolucionen conforme se alimentan de información adicional.

Entre los métodos más utilizados en *machine learning* se encuentran las máquinas de vectores de soporte (*support vector machines*), los modelos gráficos probabilísticos y las redes neuronales, tanto simples como complejas, estas últimas empleadas en el denominado *deep learning* (CEPLAN, 2021), que será abordado en el siguiente apartado.

d. *Deep learning* o aprendizaje profundo

En atención a lo señalado por el CEPLAN (2021), el *deep learning* se basa en modelos más complejos de redes neuronales artificiales y ha demostrado mejores resultados que otros métodos de aprendizaje automático, especialmente cuando hay suficientes datos y poder computacional.

Esta técnica ha sido clave en el desarrollo de sistemas de IA más sofisticados, como los modelos de procesamiento de lenguaje natural y visión por computadora. Según la UNESCO (2021), el *deep learning* surge de la combinación de algoritmos de aprendizaje automático, redes neuronales formales y el uso de macrodatos. Su arquitectura está inspirada en el funcionamiento del cerebro humano, permitiendo que los sistemas reconozcan conceptos abstractos con un mínimo de intervención humana.

Conforme a lo señalado en el Portal del Estado Peruano, se entiende por *deep learning* al método de aprendizaje similar al *machine learning*, pero más complejo, en tanto forma redes neuronales artificiales inspiradas en el cerebro humano (PCM, s. f.). De esta forma, se precisa que "estas redes pueden aprender a cumplir tareas complejas en múltiples campos de estudio" humano (PCM, s. f.).

De acuerdo con la doctrina, el *deep learning*, o aprendizaje profundo, es un subcampo del aprendizaje automático que se inspira en la estructura y función del cerebro humano, específicamente en las redes neuronales biológicas (Goodfellow *et al.*, 2016). Se caracteriza por el uso de redes neuronales artificiales con múltiples capas ocultas, lo que permite al modelo aprender representaciones de datos con diferentes niveles de abstracción (LeCun Bengio y Hinton, 2015).

A diferencia de los métodos tradicionales de aprendizaje automático que a menudo requieren una ingeniería de características manual, el *deep learning* es capaz de descubrir automáticamente las características relevantes de los datos a través de estas capas, lo que lo hace particularmente efectivo para tareas complejas como el reconocimiento de imágenes, el procesamiento del lenguaje natural y el reconocimiento de voz (LeCun *et al.*, 2015).

La capacidad de las redes neuronales profundas para aprender representaciones jerárquicas y abstractas de los datos les permite modelar relaciones intrincadas y no lineales, superando en muchos casos el rendimiento de algoritmos más superficiales (Schmidhuber, 2015). Asimismo, la efectividad del *deep learning* a menudo se ve potenciada por la disponibilidad de grandes volúmenes de datos y el poder computacional necesario para entrenar modelos complejos, lo que ha contribuido a su proliferación y éxito en diversas aplicaciones prácticas (Schmidhuber, 2015).

En síntesis, las distintas definiciones coinciden en resaltar tres elementos centrales del *deep learning*: (i) su inspiración en el funcionamiento del cerebro humano a través del uso de redes neuronales artificiales con múltiples capas; (ii) la capacidad

de dichas redes para aprender representaciones jerárquicas y abstractas de los datos sin necesidad de una ingeniería manual intensiva de características; y (iii) la dependencia de grandes volúmenes de datos y recursos computacionales para alcanzar resultados superiores frente a otros enfoques de aprendizaje automático.

e. IA Generativa (IAGen)

No todo sistema de IA constituirá IAGen, esta solamente será considerada como tal si crea contenido tal como texto, imágenes, video o audio en atención a las indicaciones realizadas por las personas.

La OCDE (2023) ha definido a IAGen como aquella "capaz de producir nuevos contenidos —como texto, imágenes, música o código— mediante el uso de modelos de IA que aprenden de grandes volúmenes de datos". En la misma línea, el Instituto Nacional de Estándares y Tecnología de los Estados Unidos (en adelante, NIST) señala que la IAGen se basa en modelos fundacionales que generan información que no estaba explícitamente presente en los datos de entrenamiento, pero que refleja los patrones estadísticos aprendidos (Instituto Nacional de Estándares y Tecnología de los Estados Unidos [NIST], 2023). La IAGen utiliza modelos entrenados con grandes cantidades de datos y es capaz de producir resultados originales que simulan creaciones humanas.

En atención a lo dispuesto en el Portal del Estado Peruano, la IAGen es considerada "un modelo de IA que permite crear contenido original como textos, imágenes, música o videos, todo partiendo de una descripción o del conjunto de datos con la que sea entrenada" (PCM, s. f.).

Conforme a lo señalado por Irazabal (2024), citando a Andrew NG, la IAGen es definida como sistemas de IA que generan contenido de alta calidad tal como texto, imagen y audio. Las IAGen adoptan *large language models* (en adelante, LLM), los cuales son una categoría de IAGen que se enfoca en la generación de texto, en ese sentido, son un subconjunto de la IAGen que se aplican para realizar tareas relacionadas con el lenguaje (Irazabal, 2024).

En conclusión, las definiciones revisadas presentan elementos comunes que permiten caracterizar a la IAGen como una categoría particular de la IA centrada en la creación de contenido "original" —textos, imágenes, música, audio o video— a partir de modelos entrenados con grandes volúmenes de datos. Su funcionamiento se basa en la identificación de patrones estadísticos complejos en los datos de entrenamiento y en la capacidad de extrapolar dichos patrones para producir resultados novedosos que imitan la creatividad humana (OCDE, 2023; NIST, 2023; Irazabal, 2024).

Además, la literatura enfatiza el rol de los modelos fundacionales, entre ellos los *large language models* (LLM), que constituyen un subconjunto especializado de la IAGen enfocado en el procesamiento y generación de lenguaje natural. En suma, la IAGen combina volumen de datos, capacidad computacional y técnicas avanzadas de modelado estadístico para situarse como una de las ramas de la IA con mayor impacto en el desarrollo tecnológico y en la transformación de múltiples sectores.

3. La IA y su relación con la privacidad y la protección de datos personales

El surgimiento de la IA y el desarrollo de sus diversos modelos y técnicas han generado impactos significativos sobre distintos derechos fundamentales. Como ha sido descrito, los derechos más afectados por las características intrínsecas de la IA son la privacidad y la protección de los datos personales. En el presente apartado, se delimitarán ambos derechos, para luego analizar cómo se ven impactados por el avance de la IA y revisar las principales iniciativas internacionales que han surgido para abordar esta problemática.

a. El derecho a la privacidad y protección de datos personales

El derecho a la privacidad, o a la intimidad, está consagrado en el artículo 2, numeral 7 de la Constitución Política del Perú. De acuerdo con Rubio *et al.* (2010), el derecho a la intimidad involucra un conjunto de actos, situaciones o circunstancias que, por su carácter personalísimo, no se encuentran normalmente expuestos al dominio público. El derecho a la intimidad se proyecta como secreto de la vida privada y como libertad: como secreto, atentan contra ella todas las intromisiones o divulgaciones ilegitimas sobre hechos relacionados con la vida privada o familiar; como libertad, la intimidad trasciende y se realiza en el derecho de toda persona a tomar por sí sola decisiones que conciernen a la esfera de su vida privada (Rubio *et al.*, 2010).

El autor enfatiza que su vulneración "se produce por la sola intromisión externa o perturbación no autorizada en las áreas privadas o reservadas (actos, hechos, hábitos, datos) que comprende, así como con la divulgación de su contenido sin contar con el consentimiento de su titular" (Eguiguren, 2000, p. 56).

Por su parte, el derecho a la protección de datos personales ha sido identificado en la doctrina constitucional como el derecho a la autodeterminación informativa (Eguiguren, 2015). Este derecho se encuentra expresamente reconocido en el numeral 6 del artículo 2 de la Constitución Política de 1993, el cual establece que

toda persona tiene derecho "a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar". Dicha disposición constitucional consagra la facultad de todo individuo de controlar el registro, uso y difusión de los datos que le conciernen, con el objetivo de resguardar su intimidad personal y familiar.

En consecuencia, este derecho implica que las personas puedan acceder a los registros en los que se almacenen sus datos, así como conocer las finalidades que justifican su conservación y la manera en que están siendo tratados. Tal como sostienen Rubio *et al.* (2010), el ejercicio de este derecho garantiza no solo la protección de la intimidad, sino también la posibilidad de supervisar activamente el flujo de información personal en manos de entidades públicas y privadas.

Si bien el derecho a la autodeterminación informativa se encuentra relacionado con la protección de la intimidad, no debe identificarse de manera estricta con el derecho a la intimidad. El Tribunal Constitucional (2002) ha precisado que, mientras el derecho a la intimidad ampara la vida privada a partir del poder jurídico de rechazar intromisiones ilegítimas en la esfera personal o familiar; el derecho a la autodeterminación informativa garantiza la facultad de toda persona de preservar dicha esfera mediante el control sobre el registro, uso y divulgación de los datos que le conciernen.

Resulta, por tanto, fundamental delimitar conceptualmente ambos derechos, no solo porque presentan matices diferenciadores; sino, también, porque ambos se encuentran entre los más afectados por el desarrollo y la aplicación de tecnologías de IA, como se expondrá a continuación.

b. La IA y la afectación a la privacidad y protección de datos: Necesidad de guías y modelos estandarizados a nivel internacional

La expansión del uso de sistemas de IA plantea importantes retos normativos en materia de privacidad y protección de datos. El desarrollo de estas tecnologías implica la recopilación y el análisis intensivo de información personal, lo cual genera interrogantes sobre la adecuación de la legislación vigente frente a estos desafíos (Guaña-Moya y Chipuxi-Fajardo, 2023). Dependiendo de sus características, esta intromisión puede derivar en una afectación directa a la intimidad de las personas o en una pérdida de control respecto de los datos de terceros utilizados en la creación y entrenamiento de sistemas de IA.

La IAGen, en particular, ha intensificado las preocupaciones. Los LLM requieren enormes volúmenes de datos para su entrenamiento y poseen la capacidad de memorizar, reproducir o inferir información personal sin el control explícito del titular (Shi *et al.*, 2024). Este uso de datos personales plantea riesgos éticos y de privacidad que deben ser cuidadosamente considerados, pues un tratamiento sin garantías adecuadas podría vulnerar derechos fundamentales.

Ante este panorama, diversas instituciones a nivel internacional y nacional han advertido la necesidad de establecer guías y modelos estandarizados para mitigar los riesgos asociados al uso de IA. En esta línea, la Comisión Europea conformó en 2019 un Grupo Independiente de Expertos que elaboró un conjunto de principios éticos para una IA fiable, basados en la supervisión humana, la transparencia algorítmica, la no discriminación y la responsabilidad (Comisión Europea, 2019).

Ese mismo año se publicó la "*Montreal Declaration for a Responsible Development of Artificial Intelligence*". Este documento fue un esfuerzo colectivo que busca aprovechar el desarrollo de la IA en beneficio del bienestar humano. Se encuentra dirigido a gobiernos, empresas y actores sociales comprometidos con una IA centrada en valores como la dignidad humana, la equidad, la sostenibilidad y la protección de derechos fundamentales (Université de Montréal, 2018).

En esa línea, la OCDE adoptó en 2019 —y actualizó en 2024— los primeros principios intergubernamentales sobre IA, que constituyen la base del trabajo de la *Global Partnership on Artificial Intelligence* (GPAI). Estos principios promueven la innovación y la confianza en la IA mediante una gestión responsable y el respeto de los derechos humanos y valores democráticos. El principio 1.2 enfatiza expresamente el deber de los actores de respetar la privacidad y la protección de datos (OCDE, 2019).

Por su parte, la UNESCO (2021) aprobó la *Recomendación sobre la Ética de la Inteligencia Artificial*, considerado el primer instrumento global orientado a promover el potencial de la IA y, al mismo tiempo, mitigar sus riesgos en materia de derechos humanos.

En el documento se enfatiza que los datos que se recopilen, usen, compartan, archiven y supriman en el marco del desarrollo de los sistemas de IA deberán realizars de forma coherente con el derecho internacional y acorde con los valores y principios de dicho documento (UNESCO, 2021). Se enfatiza que se deberán establecer marcos de protección de datos aplicados a lo largo del ciclo de vida de los sistemas de IA los cuales "deberían tomar como referencia los principios y normas internacionales de protección de datos relativos a la

recopilación, la utilización y la divulgación de datos personales y al ejercicio de sus derechos por parte de los interesados" (UNESCO, 2021).

En el ámbito regional, la Red Iberoamericana de Protección de Datos (en adelante, RIPD) publicó en 2021 su *Guía de Recomendaciones Generales para el Tratamiento de Datos en Inteligencia Artificial*, donde se exhorta a los desarrolladores a implementar políticas claras de acceso restringido, mecanismos de anonimización desde la etapa de diseño y supervisión humana en decisiones automatizadas (Red Iberoamericana de Protección de Datos [RIPD], 2021). Más recientemente, el Comité Europeo de Protección de Datos (en adelante, CEPD) ha descrito las dificultades para garantizar la privacidad en entornos de IA, especialmente ante la falta de transparencia en el uso de información personal (Comité Europeo de Protección de Datos [CEPD], 2024).

De manera más reciente, la Asamblea General de las Naciones Unidas (2024) aprobó la Resolución A/78/L.49 mediante la cual exhortó al acceso inclusivo a los beneficios de la transformación digital y al desarrollo de sistemas de IA seguros y fiables, que aseguren la protección de la privacidad y de los datos personales.

La preocupación compartida por estas entidades refleja la creciente necesidad de consolidar una gobernanza global de los datos personales y respeto de la privacidad en contextos de IA. La afectación a la privacidad no ocurre únicamente en la fase de recopilación de información, sino en distintas etapas del ciclo de vida del dato: almacenamiento, tratamiento, transferencia y uso posterior. Por ello, un análisis integral debe observar cómo los datos interactúan con los sistemas de IA a lo largo del tiempo, evaluando riesgos en cada fase, a través de sus intervinientes, agentes y cadenas de valor (Jiménez, 2024).

4. Regulación de la IA en el Perú y su relación con los estándares de privacidad y protección de datos personales

La regulación de la IA en el Perú se encuentra aún en una etapa inicial, aunque en los últimos años se han producido avances significativos. En cada uno de los pasos hacia una regulación más robusta, ha persistido como eje central la preocupación por la protección de la privacidad y de los datos personales, tal como ha ocurrido en el entorno internacional.

Esto no ha sido ignorado por las autoridades competentes. La Autoridad Nacional de Protección de Datos Personales (en adelante, ANPDP) reafirmó en 2025, durante el XXII Encuentro Iberoamericano de Protección de Datos, su compromiso con la protección de la privacidad en el marco del tratamiento masivo o a gran escala de datos personales[7]. En esa misma línea, el presente acápite analiza las principales iniciativas regulatorias referidas a la IA en el Perú, con especial énfasis en su vínculo con los estándares y preocupación por el respeto de la privacidad y protección de datos personales.

En 2021, la PCM a través de la Secretaría de Gobierno y Transformación Digital (en adelante, SGTD) publicó la Estrategia Nacional de Inteligencia Artificial (ENIA) para el periodo 2021 y 2026 (UNESCO, 2025). La Estrategia planteó como propósito que el Perú fuera reconocido como líder latinoamericano en investigación, desarrollo, innovación y adopción de la IA, promoviendo siempre su uso ético y responsable en la producción de bienes y servicios públicos y privados.

Ese mismo año, el CEPLAN (2021) publicó un reporte denominado *"Inteligencia Artificial: desafíos y oportunidades para el Perú"*. El documento tiene por objetivo brindar información sobre las tecnologías en el ámbito de la IA y su aplicación en diversos sectores en el Perú. Entre sus conclusiones, se destacó la necesidad de consolidar un marco legal sólido en materia de privacidad de datos (CEPLAN, 2021). Es más, el Documento enfatizó que "la normativa que se establezca sobre el desarrollo de la IA, principalmente para evaluar temas de privacidad y sesgos, debe ser evaluada en conjunto con especialistas de distintas disciplinas" (CEPLAN, 2021, p. 56).

En noviembre de 2021, el Perú adoptó el documento denominado *"Recomendación sobre la Ética de la Inteligencia Artificial"* propuesta por la UNESCO y citado con anterioridad. Tal como fue mencionado, el documento reconoce la privacidad como un derecho esencial para la protección de la dignidad, autonomía y capacidad de actuación de las personas (UNESCO, 2021). La adhesión a este instrumento internacional constituye un antecedente relevante, pues refleja la voluntad del Estado Peruano de alinear sus políticas nacionales con principios éticos de alcance global con especial énfasis en la privacidad y protección de datos personales.

El hito normativo más significativo a nivel nacional fue la promulgación de la Ley de IA publicada el 5 de julio de 2023. Esta norma tiene por objetivo promover el uso de la IA en el proceso nacional de transformación digital con el fin de fomentar el

7 En concordancia con lo señalado en la siguiente noticia: https://www.redipd.org/noticias/peru-promueve-y-fortalece-compromiso-internacional-en-proteccion-datos-personales

desarrollo económico y social del país[8]. A pesar de que se ha difundido que esta podría ser la primera ley de IA a nivel mundial; dicha afirmación; no es del todo precisa. En efecto, la Ley peruana ha sido comparada con el RIA, aunque existen diferencias sustanciales: mientras el reglamento europeo busca armonizar el mercado interior y es aplicable tanto a proveedores públicos como privados de sistemas de IA, la ley peruana se centra principalmente en impulsar la innovación en el sector público y establecer lineamientos generales.

Ese mismo año se aprobó la Política Nacional de Transformación Digital al 2030, que desarrolla objetivos específicos vinculados con la IA. Este documento resalta la necesidad de promover en todo momento la adopción responsable de la tecnología, con especial énfasis en la privacidad, la ética y la seguridad de los datos (Secretaría de Gobierno y Transformación Digital [SGTD], 2023).

Posteriormente, en mayo de 2024, la SGTD publicó la primera versión del Proyecto de Reglamento de la Ley de IA, seguida de una segunda en noviembre del mismo año. Con posterioridad, el 9 de setiembre de 2025, se publicó el Reglamento de la Ley de IA. Aunque este mantiene como ámbito principal de aplicación el sector público y los actores privados vinculados al Sistema Nacional de Transformación Digital, el texto contiene disposiciones que podrían extender su alcance de forma generalizada al sector privado, lo que ha generado críticas sobre eventuales conflictos de competencia e inseguridad jurídica.

Es más, en su oportunidad con los proyectos e incluso con la publicación del Reglamento de la Ley de IA, se ha cuestionado que se introducen disposiciones que exceden las competencias previstas en la Ley de IA. Esto pudo ser una de las razones por las que el 7 de abril de 2025 se presentó el Proyecto de Ley N.° 10737/2024-CR el cual tenía por objetivo la modificación de la Ley de IA. No obstante, este fue retirado en la misma fecha por un error material en la redacción del objeto de la ley. Independientemente del "error" en la redacción de la norma[9], es importante señalar que se pretendía modificar el concepto mismo de IA, así como ampliar las competencias de la SGTD. Es más, la propuesta incluía un artículo sobre "derechos humanos en entornos digitales" que enfatizaba la protección del derecho a la privacidad y protección de datos de las personas.

En línea con la Ley de IA, su reglamento reafirma el respeto de la privacidad de los datos personales en el literal b) del artículo 7, como principio rector, entendido como el respeto de forma irrestricta a la privacidad y protección de datos personales en el desarrollo, implementación y uso de la IA. Asimismo, el Reglamento de la Ley de IA enfatiza en el literal c) del mismo artículo que se garantizará el respeto y protección de los derechos fundamentales en el desarrollo, implementación y uso de sistemas basados en IA. Asimismo, se dedica un capítulo a las medidas para garantizar la transparencia y la privacidad.

Ahora bien, también existen iniciativas legislativas, mencionadas a lo largo del artículo, las cuales consideran como elemento imprescindible la protección de la privacidad y protección de datos personales. De esta forma, el Proyecto de Ley 8223/2023-CR, que propone la Ley de fomento y regulación del uso de la IA en el Perú, presentado el 14 de junio de 2024, el cual cuenta con una estructura similar a nuestra actual Ley de IA. El proyecto enfatiza la privacidad como "principio ético" a tener en cuenta en el desarrollo y uso de sistemas de IA; y, como "principio legal", la protección de los datos personales.

Junto a estas iniciativas, destacan otros proyectos de ley en discusión. El Proyecto de Ley 8223/2023-CR, presentado en junio de 2024, propone una estructura similar a la Ley de IA, pero incorpora expresamente la privacidad como principio ético y la protección de datos personales como principio legal. El proyecto incluso dedica un título completo a la materia de datos personales, aunque esta opción podría ser redundante e incluso confusa, dado que la Ley N.° 29733, Ley de Protección de Datos Personales (en adelante, LPDP), regula integralmente los derechos y obligaciones en este ámbito.

Por otro lado, el Proyecto de Ley N.° 7033/2023-CR, presentado en febrero de 2024, es quizá el más ambicioso, pues plantea una regulación aplicable tanto al sector público como al privado, definiendo expresamente los datos personales y estableciendo en su artículo 6, que los sistemas de IA deben respetar y proteger la privacidad y el tratamiento de datos de los usuarios conforme a lo dispuesto en la LPDP.

Más allá de sus diferencias, los proyectos de ley analizados coinciden en un punto común: todos

8 Esto se encuentra detallado en el artículo 1 de la Ley N.° 31814, Ley que promueve el uso de la inteligencia artificial en favor del desarrollo económico y social del país.

9 La autora del Proyecto de Ley fue la congresista María del Carmen Alva, quien consignó como objeto de la ley lo siguiente:
Artículo 1. Objeto de la ley
La presente ley tiene por objeto modificar la Ley 31814, "Ley que promueve el uso de la inteligencia artificial en favor del desarrollo económico y social del país, ***para mejorar la constitución, reconocimiento y registro de las ollas comunes; así como garantizar su financiamiento y sostenibilidad*** [Énfasis agregado].

otorgan una atención prioritaria a la protección de la privacidad y de los datos personales. Este consenso transversal se refleja también en las mesas de trabajo organizadas por la SGTD, en las que actores públicos, privados y especialistas en tecnologías emergentes han reiterado la necesidad de que la regulación peruana incorpore estándares claros en esta materia.

A la fecha de redacción del presente artículo, los proyectos legislativos mencionados no han sido aprobados o publicados oficialmente. Por ello, resultará de especial relevancia analizar la versión de los textos finales en cada una de estas iniciativas en lo relativo a la privacidad, la transparencia y la protección de datos personales, aspectos que constituyen ejes fundamentales para el diseño, desarrollo y despliegue responsable de sistemas de IA.

Ahora bien, en julio de 2025, el Instituto Nacional de Calidad (en adelante, INACAL), organismo adscrito al Ministerio de la Producción, aprobó la Norma Técnica Peruana NTP-ISO/IEC 42001:2025, primera de su tipo enfocada en establecer un sistema de gestión específico para IA. Esta norma técnica busca apoyar a las organizaciones en el desarrollo responsable de sistemas inteligentes y destaca, entre otros aspectos, el análisis de datos, la gestión del conocimiento y el aprendizaje automático (el Instituto Nacional de Calidad [INACAL], 2025).

Por último, en agosto de 2025, la SGTD publicó la Estrategia Nacional de Gobierno de Datos, en el cual se enfatiza el aprovechamiento estratégico de datos para la analítica avanzada e IA, lo cual puede mejorar la toma de decisión, predecir resultados y optimizar los servicios a la ciudadanía. Sin embargo, el documento también menciona que es imprescindible proteger y garantizar los derechos de todas las personas, que se maximicen las ventajas de la IA mientras que, a la vez, se abordan sus riesgos.

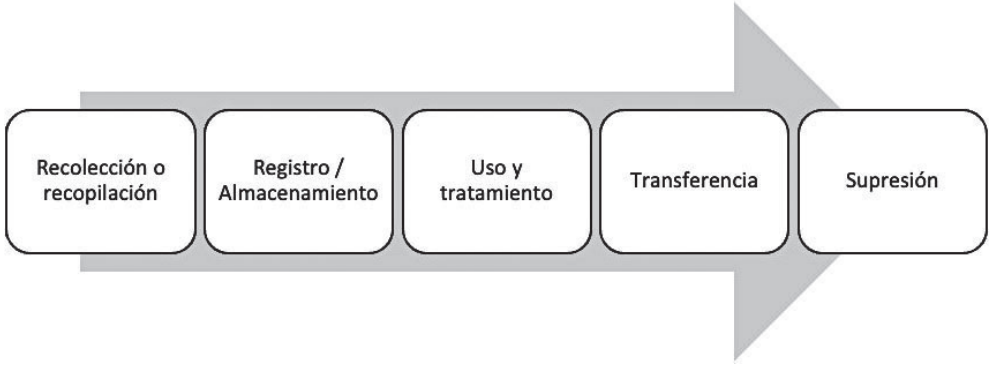
De acuerdo con la UNESCO (2025), el Perú ha mostrado avances normativos notables en materia de IA, aunque la implementación de dichos avances no ha progresado con la misma rapidez. El gran reto pendiente es articular un sistema nacional de actores, normas y procesos que, además de promover la innovación tecnológica, priorice de manera transversal el respeto de la privacidad y la protección de los datos personales como pilares del desarrollo regulatorio.

5. Recomendaciones en torno a la privacidad y protección de datos personales: El ciclo del dato en paralelo al ciclo de vida de la IA

El desarrollo y despliegue de sistemas de IA no puede desvincularse del tratamiento de datos personales, dado que estos constituyen el insumo esencial que "alimenta" los algoritmos. Sin embargo, ha sido una preocupación constante que el desarrollo de la IA, utilizando datos, sea realizado con respeto absoluto de los derechos fundamentales (Herrera, 2022). Por ello, resulta imprescindible articular el ciclo de vida de los datos personales con el ciclo de vida de la IA, de modo que la regulación, la gestión organizacional y las prácticas técnicas respondan a las exigencias de privacidad y protección de datos en cada fase del proceso, para con ello minimizar o mitigar el impacto en los derechos de las personas.

En las legislaciones sobre protección de datos personales se hace referencia al "ciclo de vida del dato personal", entendido como las distintas etapas por las que transita un dato desde su recopilación hasta su eventual eliminación, una vez cumplida la finalidad para la cual fue recolectado o el plazo de conservación correspondiente. Este enfoque permite identificar con mayor precisión los puntos críticos en los que pueden surgir riesgos para la privacidad, facilitando así la adopción de medidas adecuadas de protección. A modo ilustrativo, este ciclo incluye las siguientes fases:

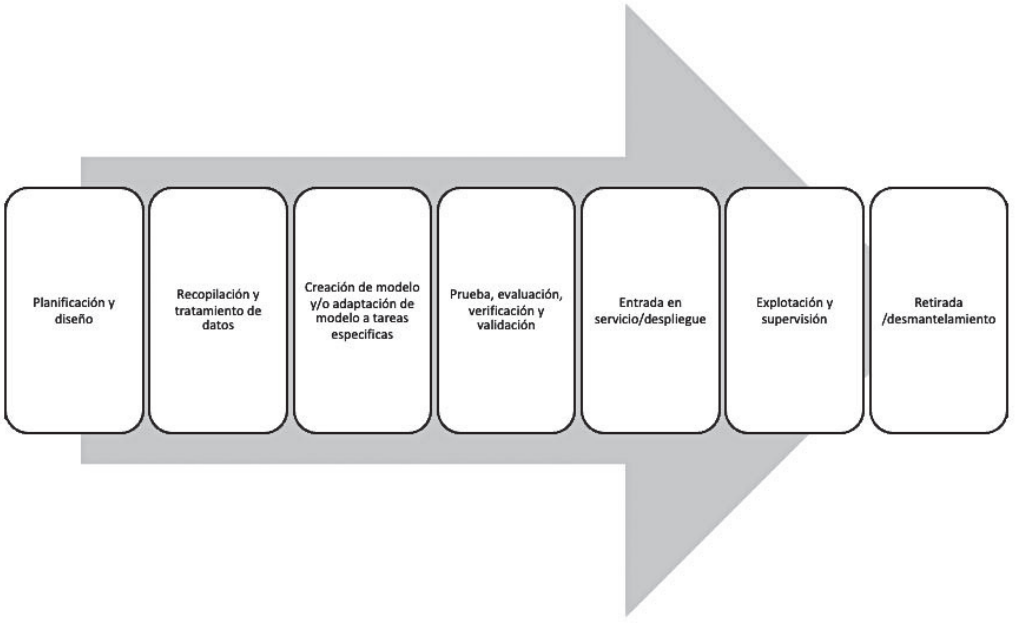
Gráfico 2. Ciclo de vida de los datos personales



Fuente: Elaboración en atención a lo dispuesto con la Agencia Española de Protección de Datos Personales (2021).

Por su parte, los sistemas de IA cuentan con su propio ciclo de vida, entendido como el conjunto de fases que atraviesa un sistema desde su concepción hasta su implementación y retirada o desmantelamiento (International Organization for Standardization [ISO], 2022). Según la OCDE (2024), el ciclo de vida de los sistemas de IA está compuesto por varias etapas las cuales son las siguientes[10]:

Gráfico 3. Ciclo de vida de los sistemas de IA



Fuente: Elaboración en base a lo dispuesto por la OCDE (2024).

Los datos personales "fluyen" durante el ciclo de vida de los sistemas de IA en muchas de sus etapas (Duffourc *et al.*, 2024, p. 244). En la fase de desarrollo, los modelos pueden ser entrenados con información personal. Posteriormente, una vez desplegados, los usuarios introducen nuevos datos personales al registrarse o interactuar con el sistema. Además, las propias salidas generadas por la IA pueden contener datos personales, ya sea de manera intencional o incidental. Finalmente, los desarrolladores pueden almacenar tanto los datos que ingresan los usuarios como los producidos por el modelo, con el fin de refinar el sistema o entrenar nuevos modelos (Duffourc *et al.*, 2024). Por este motivo, es esencial que los sistemas de IA cumplan en todo momento con los principios propios del régimen de protección de datos, desde el inicio y en cada una de sus etapas y se diseñen de manera que se proteja la privacidad (Pérez-Ugena, 2024).

La convergencia entre ambos procesos o ciclos hace evidente que cada decisión adoptada en el tratamiento de datos tenga un impacto directo en la seguridad, transparencia y ética de los sistemas de IA. Este vínculo exige que se identifiquen puntos de intersección críticos entre ambos ciclos para poder formular recomendaciones específicas que garanticen la protección de derechos fundamentales.

Adicionalmente, durante cada una de estas etapas de la vida de los sistemas de IA, intervienen diferentes agentes los cuales deberán respetar, en atención a sus propias funciones, la privacidad y protección de datos personales (Jiménez, 2024). Esto además se encuentra detallado en el RIA, en la que se describe las responsabilidades a lo largo de la cadena de valor de la IA. Si bien esta es una norma europea, considerando que es uno de los estándares primigenios sobre IA a nivel internacional, es relevante traerla a colación con el fin de considerarla en el desarrollo regulatorio peruano.

Los individuos que son mencionados en el RIA son los siguientes:

(i) Proveedor (artículo 3.3)

(ii) Responsable del despliegue (artículo 3.4)

10 A pesar que se hayan graficado la bases como una flecha secuencial, la OCDE (2024) precisó que estas fases no necesariamente lo son.

(iii) Representante autorizado (artículo 3.5)

(iv) Importador (artículo 3.6)

(v) Distribuidor (artículo 3.7)

(vi) Proveedor posterior (art. 3.68)

Los roles más importantes en el desarrollo de la vida del sistema de IA son el proveedor y el responsable del despliegue. De acuerdo con Irazabal (2024), la gran diferencia entre uno y otro es que el proveedor es quien desarrolla el sistema de IA y lo pone a disposición de los demás bajo su propio nombre, mientras que el responsable del despliegue será quien utilice el sistema de IA bajo su autoridad.

Efectivamente, el proveedor, es considerado el eje central sobre el que se disponen el mayor número de obligaciones y responsabilidades en el cumplimiento del RIA, dado que es la persona encargada de desarrollar —o mandar a desarrollar— los sistemas de IA que serán usados para la toma de decisiones (Palma, 2024). Entre sus principales obligaciones se encuentran la aplicación de medidas correctoras cuando un sistema de IA no sea conforme al RIA. Asimismo, ante la identificación de un riesgo en el sistema deberá investigar las causas de dicho riesgo e informar a las autoridades de vigilancia del mercado pertinente, facilitar la información solicitada por dichas autoridades, entre otros (Palma, 2024). En el Reglamento de la Ley de IA, se le denomina desarrollador.

Por su parte, el responsable del despliegue, al ser la persona o entidad que utilizará el sistema de IA, también cuenta con un listado extenso de obligaciones, entre las cuales se encuentran adoptar medidas técnicas y organizativas adecuadas, encomendar tareas de supervisión de los sistemas de IA, y garantizar que los datos de entrada sean pertinentes (Palma, 2024). En el Reglamento de la Ley de IA, este individuo sería principalmente el implementador o incluso usuario.

Ahora bien, considerando los diversos tipos de datos que son utilizados durante el ciclo de vida de los sistemas de IA, es plenamente viable establecer una correspondencia entre ambos "ciclos de vida". De hecho, el tratamiento de datos personales en el ciclo de vida de un sistema de IA se realiza en diversos momentos y en atención a distintas funcionalidades (Jiménez, 2024). La relación que existe entre el ciclo de vida del dato y del sistema de IA se puede representar de forma paralela, con el fin de identificar con mayor claridad los puntos en los que se deben aplicar salvaguardas jurídicas y técnicas para evitar la afectación de derechos fundamentales. Esto se puede evidenciar en el siguiente cuadro:

Fase del sistema de IA	Etapas del ciclo de vida del dato	Responsables
Planificación y diseño	Recolección Almacenamiento	Proveedor, Responsable del despliegue, Representante autorizado
Recopilación y tratamiento de datos personales	Recolección Almacenamiento Uso y tratamiento	Proveedor, Responsable del despliegue, Importador, Representante autorizado, Encargado del tratamiento (si aplica)
Creación / adaptación de modelos	Almacenamiento Uso y tratamiento	Proveedor, Responsable del despliegue, Importador, Representante autorizado
Prueba, evaluación, verificación y validación	Almacenamiento Uso y tratamiento Eliminación (de corresponder)	Proveedor, Responsable del despliegue, Importador, Representante autorizado, Encargado del tratamiento (si aplica)
Despliegue del sistema	Almacenamiento Uso y tratamiento Transferencia (de corresponder)	Responsable del despliegue, Proveedor, Importador, Distribuidor, Representante autorizado
Explotación y supervisión	Almacenamiento Uso y tratamiento Eliminación (de corresponder)	Responsable del despliegue, Proveedor, Importador, Distribuidor, Representante autorizado
Retiro / desmantelamiento	Eliminación o eventual anonimización	Responsable del despliegue, Proveedor, Importador, Distribuidor, Representante autorizado

Fuente: Elaboración propia.

Tal como se muestra en el cuadro, existe una relación directa entre las fases del ciclo de vida de la IA y las del dato personal, lo que obliga a los distintos agentes a integrar salvaguardas en cada etapa. En muchos casos, los roles pueden coincidir o solaparse, especialmente cuando varios actores determinan de manera conjunta los fines y medios del tratamiento.

En los apartados siguientes se examinarán de manera individual las principales etapas de este ciclo, identificando los riesgos más relevantes asociados al tratamiento de datos personales y a la privacidad, los responsables que intervienen en cada fase y recomendaciones específicas orientadas a mitigar la posible afectación a la privacidad y a los derechos fundamentales de las personas.

a) Planificación y diseño de los sistemas de IA: *Privacy by design and by default*

En esta fase inicial se conceptualiza el sistema de IA, se definen sus objetivos, se determinan las tareas que pretende resolver, se diseña la arquitectura y se identifican los recursos técnicos, humanos y organizativos necesarios para su desarrollo. A lo largo de esta etapa —y especialmente antes de su conclusión— los distintos actores involucrados deben garantizar que el sistema cumpla efectivamente con los objetivos, requerimientos y demás metas identificadas en la fase de inicio (ISO, 2022).

Esta etapa contempla, de forma central, la recopilación y almacenamiento de datos personales, los cuales influyen directamente en el diseño de la arquitectura y en la selección de los algoritmos que estructurarán el sistema. De acuerdo con la ISO/IEC 22989:2022, en el diseño de los sistemas de IA resulta fundamental definir las entradas de datos; los requisitos de entrenamiento y las restricciones de uso, dado que estas decisiones condicionan tanto la funcionalidad como la seguridad del sistema (ISO, 2022).

En consecuencia, tanto el proveedor —quien desarrolla o pone en el mercado el sistema de IA— como el desarrollador —quien diseña y programa el sistema— son responsables de garantizar que la planificación respete las exigencias de protección de datos y privacidad desde la concepción. Incluso el responsable del despliegue puede tener incidencia si interviene desde el inicio en la definición de los fines y medios del sistema.

Es en este punto donde adquiere especial relevancia el enfoque de "privacidad desde el diseño" (*privacy by design*), desarrollado por Ann Cavoukian en la década de 1990, que promueve la incorporación de principios de privacidad en todas las fases de concepción, operación y gestión de los sistemas (AEPD, 2019). Este enfoque fue consolidado en el artículo 25 del Reglamento (UE) 2016/679, Reglamento General de Protección de Datos de la Unión Europea (en adelante, RGPD), que obliga a los responsables del tratamiento a adoptar medidas técnicas y organizativas adecuadas para garantizar la protección de datos personales desde las fases iniciales. A ello se suma la noción de "privacidad por defecto" (*privacy by default*), la cual exige que, en ausencia de intervención del usuario, los sistemas estén configurados para ofrecer el mayor grado de protección posible (AEPD, 2020).

La aplicación de estos principios exige anticipar riesgos y asumir una responsabilidad proactiva, lo que se traduce en estrategias que integren la privacidad en todo el ciclo de vida del sistema (AEPD, 2019). Para los sistemas de IA —que suelen manejar grandes volúmenes y tipos de datos— este enfoque es indispensable. Existe un consenso relacionado a que la protección de datos debe adaptarse a la nueva realidad que impone la IA, pero de forma paralela, la IA debe, desde el diseño y por defecto, establecer procedimientos para que su aplicación sea compatible con el respeto de la privacidad y protección de datos (Herrera, 2022).

Esto además ha sido recogido en el Reglamento de la Ley de IA, cuyo artículo 29 dispone que las entidades de la Administración Pública deberán integrar la privacidad desde el diseño del sistema basado en IA, minimizando la cantidad de datos personales recopilados y utilizando técnicas de anonimización.

En este sentido, la "Guía sobre privacidad desde el diseño" de la AEPD resalta la importancia de identificar los riesgos de forma temprana y asignar roles claros de responsabilidad en la gestión de datos, mientras que la "Guía sobre protección de datos desde el diseño y por defecto" detalla controles técnicos como la anonimización, seudonimización y minimización de datos (AEPD, 2020; 2021).

Asimismo, la "Evaluación de Impacto en la Protección de Datos" constituye un instrumento esencial, especialmente para el uso de datos masivos en esta etapa del ciclo de vida del sistema de IA. Según la AEPD (2021), implica un análisis sistemático de los riesgos que el tratamiento puede generar sobre los derechos y libertades de las personas, junto con la implementación de medidas para mitigarlos.

Esta evaluación debe considerar la calidad y representatividad de los datos, los sesgos potenciales en el diseño algorítmico y los impactos de las decisiones automatizadas en los titulares. De manera concordante, la RIPD (2019) resalta la necesidad de atender a las variables que afectan los datos de entrada, las reglas algorítmicas y las decisiones de salida, ya que un tratamiento inadecuado puede comprometer la precisión, equidad y transparencia del sistema.

Esta herramienta permite identificar los posibles riesgos para los derechos y libertades de los titulares de los datos y establecer medidas de mitigación proporcionales. Durante esta etapa deben considerarse todas las dimensiones del riesgo, en tanto se definen los objetivos, funcionalidades y características técnicas del sistema. La anticipación de impactos desde el diseño no solo optimiza la funcionalidad, sino que fortalece la protección de los derechos fundamentales.

El documento denominado "Recomendaciones Generales para el Tratamiento de Datos en Inteligencia Artificial", elaborado por la RIPD, identifica aspectos clave que inciden en la gestión de riesgos algorítmicos. Entre ellos destacan la calidad y representatividad de los datos de entrada, las reglas empleadas en el diseño de los algoritmos y el impacto de las decisiones automatizadas en los derechos de las personas (RIPD, 2019):

Gráfico 4. Gestión de riesgos de los algoritmos

Fuente: Elaborado por Red Iberoamericana de Protección de Datos, 2019.

¿Es necesario realizar un análisis de riesgo relativo a la protección de datos en el Perú en el desarrollo de un sistema de IA?

Esta es una figura que ha sido desarrollada principalmente en la UE, tal como se puede evidenciar de las guías previamente citadas. No obstante, en el Perú, esta práctica ha sido incorporada normativamente. El Decreto Legislativo 1412, que aprueba la Ley de Gobierno Digital, establece en su artículo 5.3 la obligación de adoptar medidas preventivas tecnológicas, organizacionales y procedimentales en el diseño de servicios digitales. Asimismo, el artículo 40 del Nuevo Reglamento de Protección de Datos Personales, aprobado por Decreto Supremo N.° 016-2024-JUS (en adelante, Nuevo Reglamento de Protección de Datos), dispone que, de forma facultativa, se podrá realizar una evaluación de impacto relativa a la protección de datos personales.

Esta herramienta, altamente recomendable en sistemas de IA, permite anticipar riesgos, establecer medidas de mitigación proporcionales y reforzar la transparencia y rendición de cuentas. El Nuevo Reglamento de Protección de Datos recomienda la realización de la evaluación de impacto, especialmente cuando se traten datos sensibles, datos con fines de crear perfiles, o datos de personas en especial situación de vulnerabilidad. De acuerdo con su definición, la evaluación de impacto es un mecanismo de responsabilidad proactiva mediante el cual de forma previa al tratamiento de datos se analiza los riesgos que implica el tratamiento de dichos datos.

Si bien nuestra actual regulación determina que la evaluación de impacto es facultativa, considerando la cantidad y características de datos que serán utilizados por los sistemas de IA, es imprescindible realizar estos análisis. Para ello, es recomendado utilizar normas ISO o normas técnicas peruanas, las cuales incluso son mencionadas en el fraseo del Nuevo Reglamento de Protección de Datos, en tanto permiten establecer parámetros para el análisis y gestión de riesgos.

Los "riesgos" son definidos, en atención a las normas ISO, como el "efecto de incertidumbre sobre los objetivos" (ISO, 2018); y, por "gestión de riesgo", aquellas "actividades coordinadas para dirigir y controlar la organización con relación al riesgo" (ISO, 2018). Las normas ISO y las normas técnicas peruanas permiten definir lineamientos y parámetros estandarizados con el fin de que ciertas actividades se desarrollen bajo reglas comunes. Esta es una de las razones por las cuales existen normas técnicas que pretenden analizar cada una de las etapas del ciclo de vida de la IA, así como los riesgos que se pueden presentar, así como las medidas que permitirán mitigarlos.

Tal es el caso de la ISO/IEC 23894: Guía para la gestión de riesgos de IA la cual tiene por objetivo proporcionar orientación para gestionar riesgos relacionados con la IA a las organizaciones que la usan en el desarrollo, producción o implementación de diversos productos, sistemas o servicios[11]. O, tal como fue citado, en el caso peruano, la Norma Técnica Peruana NTP-ISO/IEC 42001:2025.

El propósito de la Norma Técnica Peruana es establecer requisitos y proporcionar orientación para la implementación, mantenimiento y mejora continua de un sistema de gestión de IA dentro de cualquier tipo de organización que desarrolle, provea o utilice productos o servicios con sistemas de IA (INACAL, 2025). La Norma Técnica dispone que toda organización debe identificar y documentar objetivos que permitan el desarrollo responsable de la IA. Adicionalmente, la Norma Técnica enfatiza que es necesario identificar las amenazas de seguridad a lo largo del ciclo de vida del sistema de IA tales como la contaminación de datos, robo de modelos o ataques de inversión de modelos (INACAL, 2025).

La Norma Técnica Peruana NTP-ISO/IEC 42001:2025 enfatiza este enfoque preventivo al requerir que las organizaciones adopten medidas de planificación orientadas a identificar y tratar los riesgos inherentes a los sistemas de IA. El estándar contempla acciones específicas de evaluación de riesgos, tratamiento de riesgos y evaluación de impacto de los sistemas de IA, destacando que las características propias de estos —como la capacidad de aprendizaje continuo o la falta de transparencia en sus procesos— requieren salvaguardas adicionales (INACAL, 2025). De este modo, el diseño responsable de los sistemas debe integrar la privacidad como un componente estratégico del sistema de gestión de IA.

Ahora bien, ¿cuáles son algunos de los riesgos que podríamos encontrar en esta etapa a partir de la evaluación de impacto correspondiente? Entre ellos destacan la posibilidad de sesgos algorítmicos y discriminación, cuando el algoritmo es entrenado con datos que reproducen situaciones históricas injustas; la recolección excesiva o indiscriminada de datos personales que no guardan relación con los fines del sistema (Martínez, 2019); la falta de transparencia en los criterios de diseño de los algoritmos; o la omisión de mecanismos de supervisión que garanticen la trazabilidad de las decisiones.

El análisis de riesgos y su clasificación también ha sido plasmado en el Reglamento de la Ley de IA. El artículo 22 determina que es necesario que se clasifiquen los riesgos generados por el uso de sistemas basados en IA. Es necesario que esta clasificación se realice de antemano con el fin de verificar e implementar oportunamente las medidas de mitigación que correspondan y cumplir las obligaciones pertinentes dependiendo del riesgo identificado. Esto se encuentra en concordancia con los artículos 30 y 32, los cuales determinan que, cuando un sistema basado en IA se considere de riesgo alto, será necesario realizar un análisis de impacto para identificar y minimizar riesgos potenciales.

En suma, la planificación y el diseño de sistemas de IA deben incorporar de manera obligatoria los principios de privacidad desde el diseño y por defecto, así como metodologías de gestión de riesgos y evaluaciones de impacto. Solo de este modo se podrá garantizar un desarrollo responsable que respete los derechos fundamentales, en particular la privacidad y la protección de datos personales, al mismo tiempo que se fomenta la innovación tecnológica.

b) Recopilación y tratamiento de datos: *web scraping* y controversia sobre el consentimiento

En esta etapa, como su nombre lo indica, se recurre de manera intensiva a datos, incluidos aquellos que pueden ser considerados personales de acuerdo con la normativa vigente en materia de protección de datos. Se trata de un momento crítico en el ciclo de vida de la IA, dado que en esta se identifican, seleccionan y recolectan los datos necesarios para entrenar y validar los modelos, así como para garantizar su funcionamiento operativo.

11 Esto se encuentra acorde a lo señalado en: https://tienda.aenor.com/Paginas/Noticias/isoiec-238942023,-orientacion-sobre-la-gestion-de-riesgos-en-ia.aspx?TermStoreId=30422a6b-6877-4e28-82d6-96d5dac7e3b1&TermSetId=c0c24438-f227-4594-9eb7-30942b744d4d&TermId=963fbc94-afd4-42f2-8424-971395ca7d15
Adicionalmente, existen otras normas ISO referidas a IA, las cuales enumeramos a continuación:
ISO 38507, gobernanza de la Inteligencia Artificial
ISO 25010, evaluación de calidad de los sistemas y del software de IA
ISO 42001, gestión de sistemas de Inteligencia Artificial
No obstante, a efectos del presente artículo, la más relevante es la referida a análisis de riesgos.

La procedencia de los datos puede ser muy diversa —registros administrativos, bases de datos privadas, plataformas digitales o información disponible en Internet—, lo que obliga a evaluar rigurosamente su licitud, calidad, exactitud y pertinencia. Solo así se asegura que el sistema de IA sea confiable, transparente y éticamente aceptable.

Durante esta fase participan distintos actores con responsabilidades claramente diferenciadas. El proveedor se encontrará obligado a asegurar que los datos empleados para el entrenamiento se ajusten a los principios de licitud, calidad y proporcionalidad, además de documentar los procesos de recolección y las medidas de seguridad implementadas. Junto a él se encuentra el responsable del despliegue, quien introduce el sistema en un entorno real y debe verificar que los datos empleados en la fase operativa se recojan y traten en cumplimiento estricto de la normativa nacional de protección de datos personales, asegurando además que los titulares reciban información suficiente sobre las finalidades del tratamiento.

El rol de los importadores cobra especial relevancia cuando los sistemas son adquiridos desde el extranjero, pues deben garantizar que los productos importados cumplan con las exigencias legales en el territorio de comercialización, asumiendo obligaciones equivalentes a las del proveedor. Asimismo, cuando el responsable o proveedor delega parte del tratamiento a un tercero, este último se convierte en encargado del tratamiento, figura regulada en el artículo 28 del RGPD y también reconocida en la LPDP y el Nuevo Reglamento de Protección de Datos. El encargado debe limitarse a ejecutar las instrucciones del responsable y adoptar medidas técnicas y organizativas adecuadas, sin decidir sobre las finalidades ni los medios del tratamiento.

En la práctica, los desarrolladores de IAGen suelen recurrir a grandes conjuntos de datos (*datasets*), muchos de los cuales provienen de fuentes en línea o de información "pública" obtenida mediante técnicas de *web scraping*. El *web scraping* es una técnica que se utiliza para recopilar datos de Internet y almacenarlos en una base de datos (Pacheco & Barrero, 2024). A manera de ejemplo, ChatGPT utiliza ChatGPTBot, el cual es un *crawler* que es utilizado para extraer datos y procesarlos para que el modelo sea más preciso y aumenten sus funcionalidades (Pacheco & Barrero, 2024).

Si bien este es un método que permite analizar y utilizar grandes cantidades de datos, no se encuentra exento de controversia en la medida en que el carácter público de los datos que se encuentran en Internet no implica necesariamente que su recolección y reutilización para fines de entrenamiento de modelos de IA sea lícita o compatible con el principio de consentimiento informado (AEPD, 2021).

En cuanto al marco normativo de protección de datos, tanto el RGPD como la LPDP establecen que el tratamiento solo puede realizarse con el consentimiento previo, libre, informado e inequívoco del titular, salvo en casos de excepción. En el ordenamiento peruano, estas excepciones se encuentran reguladas en el artículo 14 de la LPDP y comprenden, entre otras, el mandato legal, la satisfacción de un interés público o la ejecución de una relación contractual.

No obstante, incluso en tales escenarios subsiste la obligación de información, lo que significa que debe comunicarse de manera clara y comprensible la identidad del responsable, la finalidad del tratamiento, el tiempo de conservación de los datos, los destinatarios y los mecanismos de ejercicio de los derechos ARCO.

El cumplimiento de estas obligaciones enfrenta dificultades operativas relevantes. En particular, el tratamiento masivo de datos provenientes de múltiples fuentes heterogéneas hace casi imposible la información individualizada a cada titular. Esta problemática ha sido reconocida por la RIPD como por la Agencia Española de Protección de Datos (en adelante, AEPD), las cuales proponen la adopción de mecanismos automatizados y soluciones tecnológicas que faciliten la transparencia, la trazabilidad y la supervisión del tratamiento de datos personales en entornos de IA (AEPD, 2021; RIPD, 2021).

¿Se podrían tratar datos masivos en el marco de una excepción al consentimiento? Es importante traer a colación el concepto de "interés legítimo", que es mencionado en el RGPD. De hecho, el artículo 6 menciona que un tratamiento será lícito cuando sea necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento. Es más, el artículo 35 del RGPD dispone que en la evaluación de impacto relativa a la protección de datos se deberá incluir y considerar el interés legítimo perseguido por el responsable del tratamiento. No obstante, no se podrá perder de vista que siempre, sobre dichos intereses, no podrán prevalecer los derechos y libertades de las personas, lo cual nos coloca nuevamente en el punto de partida.

En atención a lo señalado por la AEPD (2020), el interés legítimo podría ser considerado como una alternativa de legitimación para tratamientos que requieren acceso a datos de entrenamiento, siempre que se presenten las circunstancias que permitan su utilización. No obstante, el interés legítimo también exige un mayor grado de compromiso, formalidad y competencia por parte del responsable de datos

personales para lo cual será importante evaluar el impacto en los derechos, libertades e intereses de las personas (AEPD, 2020). En ese sentido, de acreditar un interés legítimo, podría ser utilizado como una excepción al consentimiento.

¿Esto podría ser utilizado bajo estándares regulatorios peruanos? El numeral 9 del artículo 14 de la LPDP menciona a los "intereses legítimos" como excepción al consentimiento, pero en el contexto en el que el tratamiento sea necesario para salvaguardar el interés legítimo del titular de datos. Sin embargo, en el documento denominado "Estándares de Protección de Datos Personales para los Estados Iberoamericanos", elaborado por la RIPD, se menciona un supuesto que se acerca más a lo dispuesto en el RGPD, en el artículo 11, el cual dispone que será posible tratar datos cuando sean necesarios para la satisfacción de intereses legítimos perseguidos por el responsable o por un tercero, siempre que estos no prevalezcan sobre derechos y libertades.

Recordemos que el Perú es parte de la RIPD, por lo que podría ser factible utilizar dicho supuesto para el uso del *web scraping*. Sin embargo, esto deberá ser evaluado dependiendo del tipo de datos que sean utilizados para dichos fines. A manera de ejemplo, se podría utilizar el criterio del Tribunal del Noveno Circuito de Apelaciones de Estados Unidos en el caso HiQ Labs, Inc. Vs. LinkedIn Corp en el que se determinó que el *web scraping* es legal cuando son utilizados datos que se pueden acceder públicamente en Internet (Pacheco & Barrero, 2024)

En definitiva, el principio de consentimiento y el uso de datos de forma masiva es uno de los puntos más discutidos, y en los que han surgido casos y demandas que ilustran la tensión entre la necesidad de datos para el entrenamiento de modelos y el respeto a los derechos de los individuos. Un ejemplo notable es el de la compañía OpenAI y su modelo de lenguaje, ChatGPT, el cual ha sido objeto de múltiples denuncias y demandas por presunto uso indebido de datos personales a gran escala. A raíz de estas controversias, en abril de 2023, la Autoridad Francesa de Protección de Datos (CNIL) recibió al menos dos denuncias contra el chatbot de OpenAI[12]; mientras que, en Italia, la herramienta fue temporalmente bloqueada por la preocupación sobre la seguridad de los datos personales, la falta de información a los usuarios y la ausencia de un filtro de edad[13]. Según las denuncias, el modelo de IA generativa de ChatGPT, entrenado con vastos volúmenes de texto extraídos de Internet, tenía la tendencia a generar información inexacta sobre las personas, lo que contraviene el principio de exactitud del RGPD.

Las demandas no se han limitado a Europa. Un bufete de abogados de California presentó una demanda colectiva contra OpenAI alegando que la empresa "robó" información privada de cientos de millones de usuarios de internet, incluidos niños, sin su consentimiento informado. La denuncia señaló que la compañía extrajo 300,000 millones de palabras de diversas fuentes en línea, incluyendo datos de ubicación de Snapchat, información financiera de Stripe y conversaciones privadas de Slack y Microsoft Teams[14].

Es por esta razón que, adicional al principio de consentimiento, en esta fase cobran especial importancia principios adicionales como la minimización, el cual es mencionado en el RGPD y la proporcionalidad, establecido en la legislación peruana, que obligan a reducir el tratamiento de datos a aquellos que resulten estrictamente necesarios, pertinentes y adecuados para los fines previstos. De no aplicarse este principio, existe el riesgo de almacenar información innecesaria, lo que aumenta la probabilidad de daños a los titulares sin justificación válida. Asimismo, el principio de seguridad impone la obligación de establecer medidas técnicas y organizativas apropiadas, entre ellas anonimización, cifrado y controles de acceso diferenciados, todas ampliamente recomendadas por el Comité Europeo de Protección de Datos (2020) y exigibles en el Perú a través de la LPDP y el Nuevo Reglamento de Protección de Datos.

Finalmente, la normativa peruana ha desarrollado directrices específicas que refuerzan estos estándares. La Norma Técnica Peruana NTP-ISO/IEC 42001:2025, relativa a la gestión de sistemas de IA, señala que debe documentarse con detalle la adquisición y selección de datos, incluyendo su procedencia, naturaleza, volumen, categorías sensibles y finalidad, a fin de garantizar la trazabilidad del proceso (INACAL, 2025). Esta exigencia complementa el marco normativo nacional y refuerza la necesidad de que cada actor involucrado —proveedores, responsables del despliegue, importadores, representantes autorizados y encargados del tratamiento— asuma una responsabilidad activa en la recopilación y gestión de los datos personales.

En conclusión, la recopilación y el tratamiento de datos constituye un punto de intersección crítico

12 En atención a lo señalado en: https://tn.com.ar/tecno/novedades/2023/04/05/chatgpt-demandan-en-francia-a-openai-por-el-uso-abusivo-de-datos-personales/

13 En atención a lo señalado en: https://www.france24.com/es/europa/20230331-italia-bloquea-la-aplicaci%C3%B3n-de-inteligencia-artificial-chatgpt-por-razones-de-seguridad

14 En atención a lo señalado en: https://www.lavanguardia.com/tecnologia/20230702/9078189/demandan-openai-entrenar-chatgpt-datos-personales-robados-pmv.html

entre el ciclo de vida del dato y el ciclo de vida de la IA. La adecuada definición de responsabilidades y la estricta observancia de los principios de licitud, consentimiento, minimización, proporcionalidad y seguridad son condiciones indispensables para asegurar que el desarrollo de sistemas de IA respete los derechos fundamentales de los individuos.

c. Creación y/o adaptación de modelos, así como la prueba, evaluación, verificación y validación correspondiente

La fase de creación y/o adaptación de modelos constituye un momento clave en el ciclo de vida de la IA, pues se centra en el desarrollo de algoritmos y arquitecturas que permitan al sistema ejecutar las tareas definidas en la etapa de planificación. Durante este proceso, se emplean los datos previamente recopilados para entrenar y ajustar el modelo, lo que implica un tratamiento intensivo de información que puede incluir datos personales. En este sentido, tanto el proveedor como el desarrollador son responsables directos de la calidad, fiabilidad y seguridad de los modelos generados, mientras que el responsable del despliegue puede intervenir si adapta el sistema a un contexto específico o realiza ajustes para un entorno determinado. Asimismo, el importador y el representante autorizado mantienen obligaciones de verificación y cumplimiento normativo, particularmente en relación con la trazabilidad del origen de los datos y la transparencia en su utilización. El encargado del tratamiento, cuando participa en estas fases, debe garantizar que los procesos de entrenamiento, prueba y validación se realicen bajo estrictas medidas de seguridad y conforme a las instrucciones del responsable del tratamiento, sin exceder las finalidades previamente establecidas.

La ISO/IEC 22989:2022 describe esta fase como el momento en el que se materializa el diseño y desarrollo del sistema, concluyendo con un modelo listo para su verificación y validación. De acuerdo con esta norma, antes de finalizar esta etapa los actores involucrados deben asegurarse de que el sistema cumple los objetivos, requisitos y metas definidos en la fase de inicio (ISO, 2022). Ello incluye decisiones sobre la arquitectura del sistema, el código, los datos de entrenamiento y la aplicación de planes de tratamiento de riesgos en línea con la ISO/IEC 23894 (ISO, 2022).

La etapa de prueba, evaluación, verificación y validación consiste en someter los modelos a diferentes análisis para determinar su rendimiento, precisión y robustez. Estas pruebas pueden incluir evaluaciones estadísticas, análisis funcionales, simulaciones frente a posibles ciberataques o escenarios de brechas de seguridad. Su objetivo principal es asegurar que el sistema cumpla con los requisitos técnicos y legales definidos en fases previas, antes de ser desplegado en un entorno real. En esta línea, la ISO/IEC 22989:2022 destaca que la verificación y validación tienen como finalidad comprobar que el sistema funciona conforme a los requisitos, lo que exige el uso de datos de prueba distintos a los empleados durante el entrenamiento, y que, además, sean representativos de los datos reales que el sistema deberá procesar (ISO/IEC, 2022a, secc. 6.2.4).

Cuando en estas fases se utilizan datos personales, deben aplicarse mecanismos de anonimización o seudonimización siempre que sea posible, además de proceder a su eliminación una vez concluida la validación, en concordancia con lo dispuesto en el RGPD y en la LPDP. En esa línea, la NTP-ISO/IEC 42001:2025 establece que las organizaciones deben implementar procesos sistemáticos de evaluación y validación de los modelos de IA antes de su despliegue. Ello incluye actividades de monitoreo continuo, auditorías internas y revisiones por la dirección, con el objetivo de detectar desviaciones en el desempeño del sistema y asegurar que los resultados se mantengan consistentes con los criterios de calidad y responsabilidad previamente definidos (INACAL, 2025). Este enfoque reconoce que la naturaleza adaptable y evolutiva de los sistemas de IA exige validaciones periódicas, no solo al momento de su diseño inicial, sino también durante su operación.

El uso de datos personales en estas fases genera riesgos específicos. La RIPD (2021) ha destacado que, dada la necesidad de grandes volúmenes de datos en los procesos de entrenamiento y prueba, resulta imprescindible aplicar técnicas de anonimización que reduzcan al mínimo la posibilidad de identificación o reidentificación de los titulares. De lo contrario, el tratamiento puede constituir una afectación estructural a los derechos fundamentales, como lo advierte Ruschemeier (2025), al tratar información sensible sin el consentimiento adecuado o sin evaluar debidamente el principio de proporcionalidad.

Asimismo, organismos internacionales como el National Institute of Standards and Technology (en adelante, NIST) (National Institute of Standards and Technology [NIST], 2024) han advertido, además, que los sistemas de IA generativa presentan riesgos particulares para la privacidad. Entre ellos la posibilidad de que los modelos generen, infieran o incluso reproduzcan datos personales sensibles durante su entrenamiento o implementación. Por ello, el NIST recomienda implementar medidas de control preventivas, tales como evaluaciones de impacto específicas para la privacidad, auditorías continuas y mecanismos de trazabilidad tanto de los datos de entrada como de las salidas del sistema. Estas herramientas permiten detectar posibles

filtraciones de información y corregir a tiempo los riesgos asociados.

Un aspecto crítico en esta etapa es la aparición de sesgos algorítmicos. La dependencia de datos históricos puede ocasionar que los modelos reproduzcan patrones de discriminación preexistentes, afectando de manera desproporcionada a grupos vulnerables en función de criterios como género, raza, nivel socioeconómico o ubicación geográfica. Para prevenir y mitigar estos sesgos, se recomienda realizar auditorías algorítmicas periódicas que analicen el impacto de las decisiones automatizadas sobre distintos grupos poblacionales, aplicar mecanismos de trazabilidad que permitan identificar el origen de los errores y fomentar la participación de equipos multidisciplinarios en el proceso de diseño y validación. Estas prácticas han sido promovidas por la OCDE (2019), el NIST (2023) y la RIPD (2021) como pilares de una IA responsable, equitativa y respetuosa de los derechos humanos.

En esta fase también se refuerza la obligación de garantizar la seguridad de los datos, entendida como la adopción de medidas técnicas y organizativas para proteger la información frente a accesos indebidos, fugas o alteraciones. Para minimizar el riesgo de incidentes, las pruebas y validaciones suelen realizarse en entornos seguros y controlados, que deben estar aislados de los sistemas operativos, contar con protocolos de acceso restringido, mecanismos de monitoreo constante y planes de respuesta inmediata ante incidentes.

En suma, la creación, prueba y validación de modelos de IA constituye un punto de inflexión en el ciclo de vida de los sistemas, donde confluyen la necesidad de eficiencia técnica con la obligación de garantizar la privacidad y la protección de datos personales. La correcta actuación de los distintos actores involucrados —proveedor, responsable del despliegue, importador, representante autorizado y encargado del tratamiento—, junto con la aplicación de medidas de seguridad, técnicas de anonimización y auditorías algorítmicas, son condiciones indispensables para que los sistemas de IA se desarrollen de manera confiable, ética y conforme a los estándares internacionales de protección de derechos fundamentales.

d. Entrada en servicio o despliegue del sistema, así como la explotación y supervisión: Transparencia constante

La etapa de entrada en servicio o despliegue constituye el punto en el cual el sistema de IA empieza a operar en un entorno real. En este momento, el sistema se integra con aplicaciones, infraestructuras u otros procesos previamente existentes, lo que marca la transición de un desarrollo en fase experimental a una herramienta que interactúa directamente con usuarios, ciudadanos o clientes. La ISO/IEC 22989:2022 describe esta fase como el momento en el que el sistema se instala, libera o configura para su funcionamiento en un entorno objetivo, pudiendo diferenciar entre componentes de software y modelos que se despliegan de manera independiente (ISO, 2022).

En esta fase, el responsable del despliegue asume el control principal al poner en funcionamiento el sistema. Este actor se convierte, en la mayoría de los casos, en el responsable del tratamiento de los datos personales conforme al RGPD y a la LPDP, debiendo garantizar la licitud, seguridad y proporcionalidad del tratamiento de la información, así como el respeto de los derechos de los titulares. Sin embargo, el responsable del despliegue no actúa de manera aislada: el proveedor mantiene obligaciones en cuanto al soporte técnico y a las actualizaciones que resulten necesarias para corregir errores o mejorar el rendimiento del sistema. Asimismo, el importador y el distribuidor tienen responsabilidades específicas cuando intervienen en la comercialización o integración del sistema dentro del mercado nacional, mientras que el representante autorizado conserva relevancia en aquellos casos en los que el proveedor no se encuentra establecido en la Unión Europea o en el país donde se despliega el sistema. Finalmente, si el responsable o proveedor encarga parte de las operaciones de tratamiento a terceros, estos asumen la posición de encargados del tratamiento, sujetos a las instrucciones recibidas y obligados a garantizar medidas técnicas y organizativas apropiadas.

Por su parte, la fase de explotación y supervisión implica no solo el funcionamiento continuo del sistema de IA, sino también la monitorización constante de su rendimiento, la detección temprana de posibles desviaciones y la adopción de ajustes o actualizaciones. Este seguimiento es indispensable, en la medida en que los sistemas de IA pueden generar decisiones automatizadas con efectos significativos sobre las personas, lo que refuerza la necesidad de establecer un marco sólido de transparencia y supervisión.

Una de las recomendaciones esenciales en esta fase es garantizar la transparencia del sistema. El Nuevo Reglamento de Protección de Datos dispone expresamente, en su artículo 6, que el titular debe ser informado si sus datos serán objeto de decisiones automatizadas, incluidas aquellas derivadas de sistemas de IA. Esta obligación de información incluye no solo la comunicación de que se realizará un tratamiento automatizado, sino también la explicación de los criterios principales de decisión y los derechos que asisten a la persona, como la posibilidad de solicitar intervención

humana, expresar su punto de vista o impugnar la decisión adoptada.

En este sentido, los responsables del tratamiento deben ofrecer explicaciones claras, accesibles y comprensibles sobre la lógica de funcionamiento del sistema, las finalidades del tratamiento, los tipos de datos empleados y los posibles impactos de las decisiones automatizadas. Asimismo, deben habilitar canales eficaces para el ejercicio de los derechos de acceso, rectificación, cancelación, oposición y portabilidad, entendida esta última en la normativa peruana como una extensión del derecho de acceso. Dichos canales deben estar disponibles en medios físicos y digitales, garantizar la trazabilidad de las solicitudes y permitir que las respuestas se brinden dentro de los plazos previstos en la LPDP.

Asimismo, se enfatiza que la transparencia en el ámbito de la IA no puede limitarse a la publicación de información general sobre los sistemas, sino que debe asegurar un nivel de trazabilidad y explicabilidad que permita a los usuarios y supervisores entender cómo se generan las decisiones automatizadas (Vargas, 2025). Mientras que el RGPD establecía bases incipientes sobre el derecho de información y acceso, el RIA amplía este enfoque y lo traduce en una obligación para que los sistemas sean diseñados de forma que resulten comprensibles en su interacción con las personas.

Este aspecto también ha sido desarrollado en el Reglamento de la Ley de IA en su artículo 25, el cual dispone que todos los desarrolladores o implementadores de un sistema basado en IA de alto riesgo deberá establecer mecanismos para garantizar la transparencia algorítmica, con el fin de que se informe al usuario de forma previa, clara y sencilla sobre la finalidad o uso del sistema basado en IA, sus funcionalidades principales y el tipo de decisiones que puede tomar.

En este sentido, la transparencia constante supone que la organización no solo explique el funcionamiento del sistema en abstracto, sino que también garantice mecanismos de trazabilidad técnica que permitan reconstruir las decisiones adoptadas en casos concretos. Como señala Vargas (2025), la finalidad de estas obligaciones es generar confianza pública, ya que sin trazabilidad ni explicabilidad las decisiones de la IA se perciben como opacas e incontrolables. Esta aproximación normativa europea ofrece una referencia clave para el Perú, donde el reto radica en traducir el principio de transparencia en prácticas de supervisión que hagan comprensible y cuestionable el actuar de los sistemas de IA frente a los ciudadanos.

Otro aspecto crítico en esta fase son las políticas de privacidad, las cuales deben mantenerse actualizadas y redactadas en un lenguaje claro. Estas políticas deben reflejar de manera precisa cómo se gestionan los datos personales en el sistema de IA, si se transfieren a terceros y si se realizan evaluaciones o decisiones automatizadas. Además, deben revisarse periódicamente y adaptarse conforme evolucionen las funcionalidades del sistema, especialmente en casos en los que este se actualice mediante aprendizaje continuo o incorpore nuevas fuentes de datos, lo que podría modificar el alcance del tratamiento inicialmente informado.

Nuevamente, la seguridad es otro pilar esencial en la fase de explotación. Se recomienda la realización periódica de auditorías de seguridad para evaluar la eficacia de las medidas implementadas, detectar posibles vulnerabilidades y reforzar la infraestructura. De igual forma, resulta indispensable contar con planes de respuesta ante incidentes o brechas de seguridad. Dichos planes deben incluir protocolos para contener, analizar y mitigar la brecha, así como medidas de recuperación que garanticen la continuidad de las operaciones.

En cumplimiento del artículo 34 del Nuevo Reglamento de Protección de Datos, toda brecha de seguridad que involucre datos personales debe notificarse a la ANPDP dentro de las 48 horas siguientes a su detección. Además, cuando el incidente afecte de manera directa a los derechos de los titulares, debe notificarse también a estos de forma oportuna, transparente y comprensible, asegurando que puedan adoptar las medidas necesarias para proteger sus intereses.

En conclusión, la entrada en servicio, explotación y supervisión del sistema de IA demanda un enfoque de transparencia constante, sustentado en la responsabilidad proactiva de todos los actores involucrados: proveedor, responsable del despliegue, importador, distribuidor, representante autorizado y encargados del tratamiento. Solo mediante una supervisión continua, políticas de privacidad claras, mecanismos efectivos para el ejercicio de derechos y una gestión rigurosa de incidentes será posible garantizar que el uso de la IA se mantenga en armonía con los estándares legales y éticos de protección de datos personales.

e) Retirada o desmantelamiento del sistema: Eliminación definitiva de los datos

La fase de retirada o desmantelamiento constituye el cierre del ciclo de vida de un sistema de IA. Esta etapa, a menudo relegada en la práctica, reviste una importancia crítica, ya que puede implicar riesgos significativos para la privacidad y la seguridad de los datos personales tratados durante las fases previas del sistema. El retiro puede responder a múltiples razones: la obsolescencia tecnológica,

el cumplimiento de los objetivos inicialmente planteados, la decisión estratégica del responsable del tratamiento o incluso el mandato de una autoridad reguladora.

En este momento, el responsable del despliegue suele liderar el proceso, garantizando que la desactivación del sistema se realice de manera ordenada y conforme a la normativa aplicable. No obstante, el proveedor, el importador, el distribuidor y el representante autorizado pueden mantener obligaciones residuales vinculadas a la documentación, la trazabilidad y el soporte técnico para asegurar que la retirada sea completa y que no subsistan riesgos derivados del sistema. El encargado del tratamiento, cuando participe en operaciones de almacenamiento o gestión de datos, también debe ejecutar la eliminación segura conforme a las instrucciones recibidas del responsable.

Desde la perspectiva de la protección de datos, la fase de desmantelamiento se encuentra íntimamente vinculada con el principio de limitación del plazo de conservación. Tanto el RGPD (art. 5.1.e) como la LPDP establecen que los datos personales solo pueden conservarse durante el tiempo estrictamente necesario para cumplir con la finalidad para la cual fueron recolectados. Una vez concluida dicha finalidad, debe procederse a su eliminación o, en su caso, a su anonimización irreversible. Esto incluye no solo las bases de datos activas del sistema, sino también las copias de respaldo, registros de auditoría, entornos de prueba y cualquier otro archivo que contenga datos identificables.

La Guía de Recomendaciones Generales para el Tratamiento de Datos en Inteligencia Artificial elaborada por la RIPD (2021), enfatiza la necesidad de contar con un plan específico para esta etapa. Dicho plan debe contemplar medidas técnicas y organizativas dirigidas a la destrucción definitiva de los datos, garantizando que la información no pueda ser recuperada ni reconstruida. Entre las opciones disponibles se encuentran la eliminación lógica mediante algoritmos de sobreescritura segura y la eliminación física, en el caso de soportes materiales.

El proceso de eliminación debe ser además documentado de manera rigurosa, dejando constancia de aspectos como la fecha en que se realizó, los métodos utilizados, las bases de datos o repositorios eliminados y las medidas adoptadas para asegurar la imposibilidad de recuperación. Este registro constituye una evidencia indispensable para demostrar el cumplimiento del principio de responsabilidad proactiva (*accountability*) y puede ser requerido por la ANPDP en el marco de sus funciones de supervisión.

De acuerdo con la norma ISO/IEC 22989:2022, el retiro de un sistema de IA puede adoptar diversas formas: la desactivación y descarte completo cuando la finalidad para la cual fue concebido ya no subsiste, incluyendo la eliminación de los datos asociados; o bien la sustitución parcial o total del sistema cuando la finalidad se mantiene vigente, pero existe un enfoque tecnológico más adecuado para alcanzarla (ISO, 2022, sec. 6.2.9). Este estándar técnico complementa las exigencias jurídicas, al recordar que el retiro no solo es un acto de desmantelamiento, sino también de gestión responsable de la información que sustentó al sistema.

Finalmente, se recomienda que la retirada del sistema se acompañe de una auditoría de cierre, que verifique la correcta eliminación de datos y evalúe los aprendizajes obtenidos durante el ciclo de vida del sistema de IA. Este ejercicio no solo reduce los riesgos residuales, sino que también permite retroalimentar los procesos de gobernanza de la IA y mejorar las prácticas organizacionales de cara a futuros desarrollos tecnológicos.

En conclusión, la retirada o desmantelamiento de un sistema de IA no puede entenderse como un mero acto técnico, sino como una fase crucial de garantía de derechos fundamentales. La eliminación segura, definitiva y documentada de los datos personales tratados a lo largo de la vida del sistema constituye una obligación ineludible para todos los actores involucrados, y su adecuada ejecución es condición indispensable para cerrar de forma responsable el ciclo de vida de la IA.

6. ¿Es necesario abordar cada uno de estos aspectos en la regulación de IA? Retos en la fiscalización y cumplimiento de las obligaciones compartidas

Existe un consenso sobre el respeto de la privacidad y protección de datos durante todo el ciclo de vida de la IA. Ello se desprende de la lectura conjunta de las normas que regulan la IA y las normas que establecen las pautas sobre tratamiento de datos personales. A pesar de que ambos marcos regulatorios se encuentran relacionados, se debe destacar el objeto y objetivo diverso de cada una de las normas (Jiménez, 2024). De hecho, los modelos regulatorios que evalúan los riesgos de los sistemas de IA consideran que muchos de los riesgos inaceptables están relacionados con el uso indebido o desproporcionado de datos personales. No obstante, son el RIA y RGPD los que desarrollan las bases sobre las obligaciones que se desprenden para todo aquel que trata datos personales en el marco del desarrollo de los sistemas de IA.

Es indispensable comprender cómo se tratan los datos personales a lo largo del ciclo de vida de

un sistema de IA, con el objetivo de identificar los puntos críticos en los que puede haber una afectación a los derechos de los titulares y, en consecuencia, adoptar las medidas necesarias para evitarlos o mitigarlos conforme a las normas sobre protección de datos personales, todo ello considerando la particularidad de los objetivos del sistema de IA y sus características individuales. Sin embargo, consideramos que esto no implica la necesidad de regular de manera exhaustiva y directa cada uno de estos aspectos dentro de las normas generales sobre IA, especialmente por la diferencia en los objetivos en ambos cuerpos normativos.

Al contrario, una aproximación regulatoria flexible, basada en principios, puede resultar más eficaz y sostenible en el tiempo. La aplicación transversal del régimen de protección de datos personales, en combinación con la regulación de la IA, junto con la interpretación técnica especializada y las buenas prácticas internacionales, permite que los riesgos puedan abordarse sin necesidad de normar cada supuesto en detalle. En ese sentido, la creación de documentos complementarios como lineamientos, directrices técnicas o guías sectoriales resulta una vía más dinámica y actualizable, lo cual ha sido constantemente desarrollado en el entorno internacional. Esta postura ya se recoge en el Proyecto de Reglamento de la Ley de IA (2024), que señala como una de las funciones de la SGTD la aprobación de estándares y guías para el diseño, desarrollo e implementación de sistemas de IA. Estos documentos deberán ser elaborados de manera coordinada con la ANPDP, en lo que respecta a la gestión de datos personales y los derechos fundamentales vinculados.

Pretender que cada riesgo o situación potencial vinculada al tratamiento de datos personales sea incorporado directamente en una norma de carácter legal o reglamentario puede ser contraproducente. Especialmente porque las normas sobre protección de datos personales pueden ser aplicadas durante todo el ciclo de vida de los sistemas de IA (Jiménez, 2024), tal como ha sido demostrado en el presente artículo.

Las tecnologías evolucionan rápidamente, y lo que hoy es un riesgo relevante, mañana podría volverse irrelevante o transformarse en un nuevo desafío. Una regulación rígida corre el riesgo de volverse obsoleta con facilidad, lo que obligaría a modificarla constantemente, generando un esfuerzo administrativo ineficiente y ralentizando la innovación. Incluso, esto podría resultar redundante, considerando que bastará una lectura integral de las normas sobre protección de datos personales para que sean aplicables al tratamiento de datos realizado por la IA.

Ahora bien, uno de los retos centrales se encuentra en la fiscalización y sanción de conductas que contravengan las disposiciones de privacidad y protección de datos. El Nuevo Reglamento de Protección de Datos fortalece expresamente las competencias de la ANPDP, otorgándole facultades sancionadoras más claras y mecanismos de supervisión en entornos digitales complejos. En paralelo, el Reglamento de la Ley de IA prevé que la SGTD asuma un rol de autoridad técnico-normativa a nivel nacional, quien será responsable de dirigir, evaluar y supervisar el uso y la promoción del desarrollo de la IA y tecnologías emergentes. De esta forma, la SGTD deberá aprobar lineamientos, estándares y guías, entre otras disposiciones complementarias, para el desarrollo, implementación y uso de la IA, funcionando como un articulador clave en la aprobación de guías y en el monitoreo de aplicaciones de IA de alto riesgo[15]. Además, la SGTD deberá supervisar el cumplimiento de la Ley de IA y su Reglamento, pero se enfatiza que, ante incumplimiento, se pondrá en conocimiento a las autoridades correspondientes.

¿Quiénes serían estas "autoridades competentes"? Eventualmente, la ANPDP ante una contravención a las normas sobre protección de datos personales; o el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual – INDECOPI (en adelante, Indecopi), ante posibles infracciones vinculadas a los ejes temáticos de la entidad. A manera de ejemplo, si se identificara una vulneración contra los derechos de autor, esta debería ser comunicada oportunamente al INDECOPI, específicamente a la Dirección de Derechos de Autor, a fin de que inicie las acciones pertinentes.

No obstante, cabe preguntarse qué ocurriría en caso de incumplimientos de obligaciones que no tengan un correlato directo con las competencias de estas entidades. En tales supuestos, podría generarse un vacío respecto de la fiscalización y sanción de infracciones relacionadas con el desarrollo y uso de sistemas de IA. En consecuencia, surge la interrogante sobre la conveniencia de otorgar facultades de supervisión y sanción a una entidad especializada en inteligencia artificial, capaz de articular las diversas aristas técnicas, jurídicas y éticas que plantea esta tecnología.

El RIA determina un régimen de imposición de multas administrativas por parte de las autoridades de control, lo cual lo convierte en una herramienta de disuasión para el cumplimiento de las obligaciones establecidas. No contar con un régimen sancionador específico en materia de IA podría resultar contraproducente, considerando que el Reglamento de la Ley de IA en el Perú es

15 En concordancia con el literal b) del artículo 8 del Reglamento de la Ley de IA.

ambicioso en la determinación de obligaciones, cuyo cumplimiento no siempre podrá depender exclusivamente de entidades como la ANPDP o Indecopi. De hecho, la ausencia de sanciones efectivas podría generar incentivos en los que los proveedores o responsables del despliegue prioricen el desarrollo acelerado de sistemas por encima del respeto a la privacidad y la seguridad de los datos personales.

En este escenario, la discusión no se limita únicamente a la existencia de un régimen sancionador, sino también a su diseño institucional y efectividad práctica. La experiencia comparada demuestra que los marcos regulatorios de la IA deben prever mecanismos de supervisión claros, acompañados de sanciones proporcionales y disuasorias, pero también de herramientas preventivas, como auditorías periódicas, evaluaciones de impacto y protocolos de transparencia. La sola previsión de sanciones administrativas no garantiza un cumplimiento real si no se articula con políticas de gobernanza que promuevan la responsabilidad proactiva de los actores. De este modo, la regulación peruana debería avanzar hacia un modelo mixto, que combine la sanción con la prevención y que tome como referencia tanto el RIA como los estándares técnicos internacionales, a fin de lograr un equilibrio entre innovación y protección de derechos fundamentales.

En este contexto, aunque se establezca un régimen sancionador, resulta esencial garantizar una coordinación institucional sólida entre el marco normativo sobre protección de datos personales y la normativa de IA, con el fin de evitar vacíos de competencia o duplicidad de funciones. A manera de ejemplo, el Proyecto de Ley 8223/2023-CR propone un régimen de sanciones a cargo de una "Entidad Reguladora". Si esta entidad fuese la SGTD, debería delimitarse de manera clara el alcance de sus competencias frente a otros organismos, particularmente en lo relativo al tratamiento de datos personales en sistemas de IA. De no realizarse esta delimitación, podría generarse la imposición de sanciones duplicadas por los mismos hechos y fundamentos, lo cual contravendría los principios de legalidad y non bis in ídem que rigen todo procedimiento administrativo sancionador.

Asimismo, los mecanismos de fiscalización deberán adaptarse al carácter dinámico de los sistemas de IA, donde fenómenos como el *black box effect*[16] dificultan atribuir responsabilidades claras. En este punto, las normas ISO/IEC —como la 23894 (gestión de riesgos en IA) o la 42001 (sistemas de gestión de IA)— y la Norma Técnica Peruana NTP-ISO/IEC 42001:2025 ofrecen criterios técnicos verificables que podrían incorporarse como referencia obligatoria en las tareas de fiscalización. Esto permitiría que los entes supervisores no solo evalúen el cumplimiento normativo formal, sino también la idoneidad técnica de las medidas de privacidad y seguridad adoptadas por proveedores y responsables de despliegue.

Otro desafío importante es la armonización con los estándares internacionales. El RIA y las guías de la OCDE, UNESCO, ONU, entre otros, sobre IA responsable constituyen referentes imprescindibles para el Perú, no solo porque elevan el estándar de protección, sino porque en un entorno globalizado, la interoperabilidad normativa es esencial para el comercio digital y la transferencia de datos transfronterizos. En este sentido, las futuras directrices nacionales deben asumir explícitamente la compatibilidad con dichos marcos, incorporando buenas prácticas internacionales que fortalezcan la seguridad jurídica y la confianza en el ecosistema digital.

Finalmente, la supervisión no debería limitarse a una función sancionadora, sino también tener un enfoque preventivo y de acompañamiento técnico. Ello implica que la ANPDP y la SGTD desarrollen mecanismos de asesoría, auditorías preventivas y programas de capacitación en privacidad desde el diseño, dirigidos tanto a entidades públicas como a desarrolladores privados. De este modo, se consolidaría una fiscalización progresiva, que garantice la tutela efectiva de los derechos sin frenar la innovación tecnológica.

7. Conclusiones

La IA y la protección de datos personales mantienen una relación de interdependencia estructural. El tratamiento de datos constituye el insumo esencial para el diseño, entrenamiento, despliegue y supervisión de los sistemas de IA y, en la mayoría de los casos, estos datos son personales. Por este motivo, las normas sobre protección de datos personales son de plena aplicación a todo el ciclo de vida de los sistemas de IA y a su cadena de valor, siendo el cumplimiento de la regulación sobre datos y privacidad un cimiento de una IA ética (Jiménez, 2024). De allí que la gestión responsable de la información no solo sea un requisito legal, sino una condición necesaria para garantizar la legalidad, legitimidad y confiabilidad de la IA.

En el contexto peruano, la Ley de IA, el Reglamento de la Ley de IA, los proyectos de ley y los recientes instrumentos de política pública —como la Estrategia Nacional de Inteligencia Artificial o la

16 El "efecto caja negra" en la IA se refiere a la dificultad de entender cómo o por qué un sistema de IA llega a una decisión o resultado particular, a causa de que los algoritmos utilizan reglas que pueden ser muy complejas para ser comprendidas o porque es imposible determinar con exactitud los factores que fueron utilizados para llegar a una decisión (Van Kolfschooten, 2022).

Política Nacional de Transformación Digital al 2030— reconocen expresamente el protagonismo de la privacidad y de la protección de datos personales en el desarrollo tecnológico. Sin embargo, el tratamiento masivo y heterogéneo de datos que caracteriza a la IA plantea tensiones con principios fundamentales de la normativa vigente, tales como el consentimiento previo, libre e informado; la finalidad específica; la proporcionalidad; y el deber de información. Estas tensiones exigen replantear la forma en que tales principios se aplican a entornos dinámicos, automatizados y altamente complejos.

El análisis efectuado en este trabajo evidencia que cada etapa del ciclo de vida de la IA guarda correspondencia con fases específicas del ciclo de vida del dato personal. La planificación y diseño requieren la incorporación obligatoria de los principios de *privacy by design* y *privacy by default*; la recopilación y tratamiento de datos demandan un escrutinio riguroso de la licitud de las fuentes y del consentimiento; la creación, prueba y validación de modelos exigen evaluaciones de impacto, anonimización y mitigación de sesgos; el despliegue y supervisión requieren transparencia activa; mientras que la retirada o desmantelamiento impone la eliminación segura y definitiva de los datos. Esta correlación refuerza la idea de que la regulación de IA debe complementarse con marcos robustos de protección de datos, aplicables de forma transversal.

Asimismo, la experiencia internacional demuestra que la regulación excesivamente rígida puede volverse obsoleta en plazos cortos frente al ritmo de la innovación tecnológica. Por ello, resulta más eficaz combinar normas generales con instrumentos flexibles: guías técnicas, directrices sectoriales, normas técnicas como la NTP-ISO/IEC 42001:2025 y estándares internacionales como la ISO/IEC 22989:2022 o la ISO/IEC 23894:2023. Estos proporcionan metodologías prácticas para gestionar riesgos, establecer salvaguardas y asegurar que la protección de datos se integre desde el diseño hasta la fase final del sistema.

En este escenario, las normas técnicas juegan un papel crucial como puentes entre los principios normativos y la implementación práctica. Al proporcionar criterios verificables y estandarizados, permiten a las organizaciones desarrollar sistemas de IA bajo parámetros homogéneos de calidad, seguridad y respeto a la privacidad. La adopción de la NTP-ISO/IEC 42001:2025 por parte del Perú constituye un avance significativo, pues establece un marco de gestión que obliga a identificar riesgos, documentar procesos y aplicar controles de seguridad durante todo el ciclo de vida de los sistemas de IA. Esta norma, complementada por lineamientos internacionales, se convierte en una herramienta esencial para garantizar que la innovación tecnológica no se produzca en detrimento de los derechos fundamentales.

Además, la utilización de normas técnicas facilita la supervisión y fiscalización por parte de las autoridades competentes. Al definir estándares objetivos, estas normas permiten que tanto los desarrolladores como los responsables del despliegue acrediten el cumplimiento de obligaciones regulatorias mediante auditorías y certificaciones. Esto no solo refuerza la transparencia y la rendición de cuentas, sino que también genera confianza en la ciudadanía y en el mercado, lo cual resulta indispensable para consolidar un ecosistema de IA confiable y sostenible. En ese sentido, la integración de normas técnicas nacionales e internacionales debe ser concebida como un eje estratégico en la construcción de un marco regulatorio peruano coherente y alineado con las mejores prácticas globales.

Finalmente, una adecuada articulación entre la regulación de IA y el marco de protección de datos personales en el Perú no debe orientarse a la sobrerregulación, sino a la consolidación de principios claros, mecanismos efectivos de supervisión y herramientas dinámicas que permitan la adaptación constante. El reto está en garantizar que la innovación tecnológica se desarrolle de manera responsable, maximizando sus beneficios sociales y económicos, al tiempo que se preservan los derechos fundamentales de las personas. Solo bajo este equilibrio será posible construir una gobernanza de la IA que sea sostenible, legítima y respetuosa de la dignidad humana.

Lista de referencias

Agencia Española de Protección de Datos. (2019, octubre). *Guía de privacidad desde el diseño*. https://www.aepd.es/guias/guia-privacidad-desde-diseno.pdf

Agencia Española de Protección de Datos. (2020, febrero). *Adecuación al RGPD de tratamientos que incorporan inteligencia artificial: Una introducción*.

Agencia Española de Protección de Datos. (2020, octubre). *Guía de protección de datos por defecto*.

Agencia Española de Protección de Datos. (2021). *Gestión del riesgo y evaluación de impacto en tratamientos de datos personales*. https://www.aepd.es/guias/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf

Agencia Española de Protección de Datos. (2021, enero). *Requisitos para auditorías de tratamientos que incluyan IA*.

Agencia Española de Protección de Datos. (2024). *La AEPD recibió 19.000 reclamaciones en 2024, con*

la IA, los espacios de datos y los neurodatos entre los retos prioritarios. https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/aepd-recibio-19000-reclamaciones-con-ia-espacios-de-datos-y-neurodatos-entre-retos-prioritarios

Asamblea General de las Naciones Unidas. (2024). *Aprovechar las oportunidades de sistemas seguros, protegidos y fiables de inteligencia artificial para el desarrollo sostenible* (Resolución A/78/L.49). Naciones Unidas. https://docs.un.org/es/A/RES/78/265

Blanes Jover, J. (2025). El concepto de inteligencia artificial en el Reglamento de la Unión Europea. En I. Sánchez Frías & Y. Villegas Almagro (dirs.), *Derecho y entornos digitales* (pp. 31-48).

Castelvecchi D. (2016) Can we open the black box of AI? *Nature, 538* (7623), 20-23. https://doi.org/10.1038/538020a

Cavoukian, A. (2009). *Privacy by design: The 7 foundational principles*. Information and Privacy Commissioner of Ontario. https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

Centro Nacional de Planeamiento Estratégico. (2021). *Inteligencia artificial: desafíos y oportunidades para el Perú*. CEPLAN.

Comisión Europea. (2018). *Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: Inteligencia artificial para Europa* (COM (2018) 237 final). Oficina de Publicaciones de la Unión Europea. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52018DC0237

Comisión Europea. (2019). *Ethics guidelines for trustworthy AI*. https://digital-strategy.ec.europa.eu/es/library/ethics-guidelines-trustworthy-ai

Congreso de la República del Perú. (2023). Ley N.º 31814. *Ley que promueve el uso de la inteligencia artificial en favor del desarrollo económico y social del país*. Diario Oficial El Peruano.

Congreso de la República del Perú. (2024). Proyecto de Ley N.º 7033/2023-CR. *Ley que regula el desarrollo y uso de la inteligencia artificial en el Perú*. https://www.congreso.gob.pe/

Congreso de la República del Perú. (2024). Proyecto de Ley N.º 8223/2023-CR. *Ley de fomento y regulación del uso de la inteligencia artificial en el Perú*. https://www.congreso.gob.pe/

Congreso de la República del Perú. (2025). Proyecto de Ley N.º 10737/2024-CR. Retirado el mismo día de su presentación. https://www.congreso.gob.pe/

Duffourc, M. N., Gerke, S., & Kollnig, K. (2024). Privacy of personal data in the generative AI data lifecycle. *New York University Journal of Intellectual Property and Entertainment Law, 13*(2), 219-268. https://jipel.law.nyu.edu/privacy-of-personal-data-in-the-generative-ai-data-lifecycle/

EDPB. (2023). *Statement on the use of personal data in the training of AI systems*. Comité Europeo de Protección de Datos.

Eguiguren Praeli, F. (2000). La libertad de información y su relación con los derechos a la intimidad y al honor en el caso peruano. *IUS ET VERITAS, 10*(20), 51–75. https://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/15924

Eguiguren Praeli, F. J. (2015). El derecho a la protección de los datos personales: Algunos temas relevantes de su regulación en el Perú. *THĒMIS-Revista de Derecho, 67*, 131–140. https://revistas.pucp.edu.pe/index.php/themis/article/view/14462

European Commission. (2023). *Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206

France 24. (2023, 31 de marzo). *Italia bloquea la aplicación de inteligencia artificial ChatGPT por razones de seguridad*. France 24. https://www.france24.com/es/europa/20230331-italia-bloquea-la-aplicaci%C3%B3n-de-inteligencia-artificial-chatgpt-por-razones-de-seguridad

Goodfellow, I., Bengio, Y. & Courville, A. (2016). *Deep learning*. MIT Press.

Guaña-Moya, J., & Chipuxi-Fajardo, L. (2023). Impacto de la inteligencia artificial en la ética y la privacidad de los datos. *RECIAMUC*, *7*(3), 927–940. Herrera de las Heras, R. (2022). *Aspectos legales de la inteligencia artificial. Personalidad jurídica de los robots, protección de datos y responsabilidad civil*. Dykinson S.L.

Instituto Nacional de Calidad (INACAL). (2025). *Norma Técnica Peruana NTP-ISO/IEC 42001:2025. Sistemas de gestión de inteligencia artificial. Requisitos con orientación para su uso*.

International Organization for Standardization. (2018). *ISO 31000:2018 Risk management — Guidelines*. ISO. https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es

International Organization for Standardization. (2022). *ISO/IEC 22989:2022 Information technology — Artificial intelligence — Artificial intelligence concepts and terminology*. ISO.

International Organization for Standardization. (2023). *ISO/IEC 23894:2023 Information technology — Artificial intelligence — Guidance on risk management*. ISO.

Irazabal Arana, E. (2024). *La inteligencia artificial explicada para abogados* (2.ª ed.). LA LEY Soluciones Legales.

Iturmendi Rubia, J. M. (2024). Inteligencia artificial y derechos humanos: Desafíos y oportunidades en la era digital. Introducción al monográfico. *Revista Deusto de Derechos Humanos,* (14), 11-31.

Jiménez López, J. (2024). El Reglamento de inteligencia artificial y el Reglamento general de protección de datos. En L. Cotino Hueso & P. Simón Castellano (dirs.), *Tratado sobre el Reglamento de Inteligencia Artificial de la Unión Europea* (pp. 149–178). Aranzadi.

LeCun, Y., Bengio, Y. & Hinton, G. (2015). Deep learning. *Nature*, *521*(7553), 436–444.

Martínez Devia, A. (2019). *La inteligencia artificial, el big data y la era digital: una amenaza para los datos personales*. *Revista Propiedad Intelectual, 27,* 49-65

Ministerio de Justicia y Derechos Humanos del Perú. (2011). Ley N.º 29733. *Ley de Protección de Datos Personales*. Diario Oficial El Peruano.

Ministerio de Justicia y Derechos Humanos del Perú. (2018). Decreto Legislativo N.º 1412. *Ley de Gobierno Digital*. Diario Oficial El Peruano.

Ministerio de Justicia y Derechos Humanos del Perú. (2023, enero 29). *Perú promueve y fortalece compromiso internacional en la protección de datos personales*. https://www.gob.pe/institucion/minjus/noticias/1195010-peru-promueve-y-fortalece-compromiso-internacional-en-la-proteccion-de-datos-personales

Ministerio de Justicia y Derechos Humanos del Perú. (2024). Decreto Supremo N.º 016-2024-JUS. *Nuevo Reglamento de la Ley de Protección de Datos Personales*. Diario Oficial El Peruano.

Ministerio de la Producción. (2025, 9 de julio). *INACAL aprueba la primera Norma Técnica Peruana sobre sistemas de gestión de inteligencia artificial*. https://www.gob.pe/institucion/produce/noticias/1205830-inacal-aprueba-la-primera-norma-tecnica-peruana-sobre-sistemas-de-gestion-de-inteligencia-artificial

Montreal Declaration. (2018). *Declaración de Montreal para un desarrollo responsable de la inteligencia artificial*. https://declarationmontreal-iaresponsable.com/

NIST (National Institute of Standards and Technology). (2023). *NIST Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf

Organisation for Economic Co-operation and Development (OECD). (s. f.). *About GPAI*. OECD.AI. https://oecd.ai/en/about/about-gpai

Organisation for Economic Co-operation and Development (OECD). (s. f.). *OECD.AI policy observatory: Dashboard overview*. https://oecd.ai/en/dashboards/overview

Organisation for Economic Co-operation and Development (OECD). (2019). *OECD principles on artificial intelligence*. OECD.AI. https://oecd.ai/en/ai-principles

Organisation for Economic Co-operation and Development (OECD). (2019). *Recommendation of the Council on Artificial Intelligence*. OECD Legal Instruments. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

Organisation for Economic Co-operation and Development (OECD). (2023). *Generative AI: Opportunities and risks*. *OECD Digital Economy Papers, No. 343*. OECD Publishing. https://doi.org/10.1787/5aaa3e6a-en

Organisation for Economic Co-operation and Development (OECD). (n. d.). *Artificial intelligence*. OECD. https://www.oecd.org/en/topics/artificial-intelligence.html

Pacheco Chaparro, J. M. & Barrero Ramírez, L. (2024). Implicaciones legales del web scraping en el entrenamiento de modelos de inteligencia artificial generativa. *Revista La Propiedad Inmaterial*, (38), 167–189. https://doi.org/10.18601/16571959.n38.07

Palma Ortigosa, A. (2024). *Régimen general de obligaciones de proveedores y responsables del despliegue en el Reglamento de inteligencia artificial*. En L. Cotino Hueso & P. Simón Castellano (dirs.), *Tratado sobre el Reglamento de Inteligencia Artificial de la Unión Europea* (pp. 447–471). Aranzadi.

Parlamento Europeo. (2020, 20 de octubre). *Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas (2020/2012(INL)) [Resolución 2020/0275]*. https://www.europarl.europa.eu/doceo/document/TA-9-2020-0275_ES.html

Parlamento Europeo y Consejo de la Unión Europea. (2024). *Reglamento (UE) 2024/1689 del Parlamento*

Europeo y del Consejo relativo a la inteligencia artificial. Diario Oficial de la Unión Europea.

Pérez-Ugena Coromina, M. (2024). Protección de datos en la aplicación de sistemas de inteligencia artificial. *Revista Anuario Parlamento y Constitución*, (25), 207–232. https://doi.org/10.71206/rapc.393

Presidencia del Consejo de Ministros. (2021). *Recomendaciones de uso ético de la inteligencia artificial (IA)*. https://www.gob.pe/69865-recomendaciones-de-uso-etico-de-la-inteligencia-artificial-ia

Presidencia del Consejo de Ministros. (s. f.). *¿Qué es la inteligencia artificial (IA)?*. Gobierno del Perú. https://www.gob.pe/69730-que-es-la-inteligencia-artificial-ia

Presidencia del Consejo de Ministros. (s. f.). *Inteligencia artificial*. Gobierno del Perú. https://www.gob.pe/es/institucion/pcm/tema/19283-inteligencia-artificial

Presidencia del Consejo de Ministros - Secretaría de Gobierno Digital. (2021). *Estrategia Nacional de Inteligencia Artificial 2021–2026*. https://www.gob.pe/institucion/pcm/informes-publicaciones/2563585

Presidencia del Consejo de Ministros - Secretaría de Gobierno y Transformación Digital. (2024). *Proyecto de Reglamento de la Ley de IA* (segunda versión). https://www.gob.pe/pcm

Red Iberoamericana de Protección de Datos. (2019). *Recomendaciones generales para el tratamiento de datos en inteligencia artificial*. https://www.redipd.org/sites/default/files/2023-05/recomendaciones-inteligencia-artificial-red-ipd.pdf

Rubio, M., Eguiguren, F. & Bernales, E. (2010). *Los derechos fundamentales en la jurisprudencia del Tribunal Constitucional: Análisis de los artículos 1, 2 y 3 de la Constitución*. Fondo Editorial PUCP.

Ruschemeier, H. (2025). Generative AI and data protection. In *Cambridge Forum on AI: Law and Governance* (vol. 1). Cambridge University Press (CUP). https://doi.org/10.1017/cfl.2024.2

Schmidhuber, J. (2015). Deep learning in neural networks: An overview. *Neural Networks*, *61*, 85–117.

Shahriar, S., Allana, S., Hazratifard, S.M. & Dara, R. (2023). A Survey of Privacy Risks and Mitigation Strategies in the Artificial Intelligence Life Cycle. *IEEE Access,* 11, 61829-61854.

Secretaría de Gobierno y Transformación Digital. (2023). *Política Nacional de Transformación Digital al 2030*. https://cdn.www.gob.pe/uploads/document/file/4932850/Pol%C3%ADtica%20Nacional%20de%20Transformaci%C3%B3n%20Digital%20al%202030.pdf?v=1691014709

Secretaría de Gobierno y Transformación Digital. (2025). *Estrategia Nacional de Gobierno de Datos*. Presidencia del Consejo de Ministros. https://cdn.www.gob.pe/uploads/document/file/8572678/7097112-estrategia-nacional-de-gobierno-de-datos.pdf?v=1756498854

Shi, Y., Wang, W. & Huang, Y. (2024). Privacy issues and strategies in generative artificial intelligence. *Information, 15*(11), 697. https://doi.org/10.3390/info15110697

Statista. (2025). *Global AI market size forecast 2024–2030*. Statista. https://www.statista.com/forecasts/1474143/global-ai-market-size

Todo Noticias. (2023, 5 de abril). *ChatGPT: demandan en Francia a OpenAI por el uso abusivo de datos personales*. TN. https://tn.com.ar/tecno/novedades/2023/04/05/chatgpt-demandan-en-francia-a-openai-por-el-uso-abusivo-de-datos-personales/

Tribunal Constitucional del Perú. (2002). *Sentencia 1797-2002-HD/TC*.

UNESCO (Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura). (2021). Recomendación sobre la Ética de la Inteligencia Artificial. https://unesdoc.unesco.org/ark:/48223/pf0000381137

Université de Montréal. (2018). *Montreal Declaration for a Responsible Development of Artificial Intelligence*. https://recherche.umontreal.ca/english/strategic-initiatives/montreal-declaration-for-a-responsible-ai/

Van Kolfschooten, H. (2022). EU regulation of artificial intelligence: Challenges for patients' rights. *Common Market Law Review, 59*(1), 81–112. Kluwer Law International.

Vargas Martínez, P. (2025). La evolución de los conceptos de transparencia y explicabilidad: De los años 90 al Reglamento de Inteligencia Artificial. En I. Sánchez Frías & Y. Villegas Almagro (dirs.), *Derecho y entornos digitales* (pp. 49-70). Atelier Libros Jurídicos.

Zhang, D., Xia, B., Liu, Y., Xu, X., Hoang, T., Xing, Z., Staples, M., Lu, Q. & Zhu, L. (2024). Privacy and copyright protection in generative AI: A lifecycle perspective. In *Proceedings of the IEEE/ACM 3rd International Conference on AI Engineering - Software Engineering for AI* (pp. 92–97). ACM. https://doi.org/10.1145/3644815.3644952