CELE
Centro de Estudios en Libertad de Expresión

Informe Legislativo

18

Perú – La regulación de la inteligencia artificial: análisis de la Ley N.° 31814 y su reglamento en perspectiva comparada

CELE

Junio 2026

Facultad de Derecho

Centro de Estudios en Libertad de Expresión

UP
Universidad de Palermo

La regulación de la inteligencia artificial en el Perú: análisis de la Ley N.° 31814 y su reglamento en perspectiva comparada

CELE/UP

celeupalermo@gmail.com

15 de junio de 2026

Introducción

La regulación de la inteligencia artificial (IA) se ha convertido en una prioridad creciente para los sistemas jurídicos contemporáneos. A nivel global, el debate sobre cómo encuadrar normativamente el desarrollo y despliegue de sistemas basados en IA ha adquirido especial urgencia ante la proliferación de tecnologías capaces de incidir directamente en el ejercicio de derechos fundamentales, como la privacidad, la no discriminación, la libertad de expresión y la autonomía individual. En este contexto, la Unión Europea adoptó en 2024 el Reglamento de Inteligencia Artificial (AI Act), considerado el marco regulatorio más comprensivo desarrollado hasta la fecha[1].

En América Latina, Perú se ha posicionado como el primer país en establecer un marco legal específico para la IA mediante la promulgación de la Ley N.° 31814 en 2023 y su reglamento, el Decreto Supremo N.° 115-2025-PCM, aprobado en 2025. Si bien este marco normativo constituye un avance relevante en la institucionalización de la gobernanza de la IA en la región, su diseño presenta ciertas ambigüedades conceptuales y vacíos regulatorios que podrían dar lugar a interpretaciones restrictivas de derechos fundamentales. Estas tensiones se manifiestan particularmente en ámbitos como la libertad de expresión, el anonimato en el espacio público y los límites al uso estatal de tecnologías de vigilancia.

---

[1] Comisión Europea. (2024). *Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (Reglamento de Inteligencia Artificial)*. Diario Oficial de la Unión Europea; González, M., Pérez, A. y Palacios, L. (2025). *Gobernanza global de la IA: ¿quién regula, con qué enfoque y para quién?* (Artículo de investigación no. 67). https://www.palermo.edu/Archivos_content/2025/cele/junio/05_2025_AI_67_.pdf

El reglamento de la ley peruana de inteligencia artificial

El texto de la Ley N.° 31814 establece de manera general los principios por los que se debe regir el desarrollo y uso de la inteligencia artificial, así como los que gobiernan su supervisión en manos de la Secretaría de Gobierno y Transformación Digital. Sin embargo, el contenido regulatorio más importante y detallado en materia de inteligencia artificial se encuentra en el Decreto Supremo N.° 115-2025-PCM, que contiene el reglamento de la ley. Por ello, el presente análisis girará en torno a este texto principalmente.

Este reglamento adopta un enfoque regulatorio basado en riesgos, siguiendo en términos generales el modelo desarrollado por el AI Act europeo. En este esquema se establecen dos categorías principales de riesgos: por un lado, los usos indebidos de la IA, que quedan expresamente prohibidos por el artículo 23.1; y, por otro, los sistemas de alto riesgo, que están sujetos a requisitos regulatorios reforzados, relacionados a transparencia algorítmica (artículo 25), evaluación de riesgos potenciales a derechos fundamentales (artículo 30) y supervisión humana (artículo 31.4). Dichos requisitos, además, deben sumarse a aquellos establecidos para el desarrollo o implementación de sistemas de IA independientemente de su nivel de riesgo: El cumplimiento de garantías de protección de datos personales (artículo 26) y de principios éticos en el diseño y operación de los sistemas (artículo 27).

En cuanto a la supervisión del cumplimiento de este reglamento, esta función ha sido atribuida, como se mencionó antes, a la Secretaría de Gobierno y Transformación Digital (SGTD), a través de la Subsecretaría de Tecnologías y Seguridad Digital (SSTSD) y del Centro Nacional de Seguridad Digital (CNSD) (Ley N.° 31814, artículo 4).

Análisis crítico: vacíos, ambigüedades y riesgos del marco regulatorio

La vaguedad conceptual en la prohibición de manipulación de decisiones

El artículo 23.1 del Decreto Supremo N.° 115-2025-PCM prohíbe los sistemas basados en IA destinados a influir de manera engañosa o manipulativa en la toma de decisiones de las personas, en particular cuando empleen técnicas subliminales o deliberadamente engañosas, o cuando aprovechen vulnerabilidades cognitivas, emocionales o socioeconómicas con el objetivo de modificar de manera sustancial el comportamiento de los individuos.

Sin embargo, la disposición no establece con claridad la frontera entre manipulación prohibida y formas legítimas de persuasión. Esta distinción es conceptualmente compleja. En

la literatura filosófica y jurídica, la manipulación suele definirse como una forma de influencia que elude o distorsiona la capacidad racional del sujeto[2]. No obstante, en el contexto de los sistemas algorítmicos contemporáneos, esta definición puede resultar difícil de operacionalizar. Es por ello que el debate reciente sobre la prohibición de la manipulación usando inteligencia artificial se inserta en un debate contemporáneo más amplio sobre la personalización algorítmica de contenidos y el perfilamiento en redes sociales. Algoritmos de recomendación de noticias, sistemas de publicidad política segmentada o asistentes conversacionales que promueven determinadas posturas podrían, en determinadas circunstancias, quedar comprendidos dentro de una definición amplia de manipulación, dependiendo del criterio interpretativo adoptado por la autoridad competente.

La indeterminación conceptual en normas sancionatorias o prohibitivas, como las que se explicarán en la sección siguiente, plantea problemas relevantes desde la perspectiva del principio de legalidad. Además, puede generar efectos de enfriamiento (chilling effects) sobre actividades legítimas de comunicación, innovación tecnológica o debate público. El derecho comparado ofrece algunos elementos para mitigar este tipo de ambigüedades: el AI Act europeo, como se examinará en la sección 4, utiliza criterios más delimitados y técnicamente precisos para definir las técnicas subliminales prohibidas.

La vigilancia masiva con base legal

El artículo 23.1.c del Decreto Supremo N.° 115-2025-PCM prohíbe la vigilancia masiva cuando esta se realice sin base legal o cuando genere —o pueda generar— un impacto desproporcionado en el ejercicio de derechos fundamentales. Sin embargo, la disposición introduce una excepción significativa: la vigilancia masiva podría resultar admisible cuando exista una base legal que la autorice.

Este diseño normativo plantea interrogantes importantes desde la perspectiva de las garantías de derechos fundamentales. La mera existencia de una base legal no constituye necesariamente una salvaguarda suficiente frente al uso de tecnologías de vigilancia mediadas por IA para monitorear el discurso político, el activismo o la participación ciudadana. En el caso peruano, el Congreso ha aprobado en diversas ocasiones normas que habilitan prácticas de vigilancia cuya compatibilidad con los estándares internacionales de derechos humanos ha sido objeto de cuestionamientos.

---

[2] Noggle, R. (1996). Manipulative actions: A conceptual and moral analysis. *American Philosophical Quarterly, 33*(1), 43-55.

Existen antecedentes documentados de vigilancia digital dirigida contra activistas y ciudadanos[3]. Asimismo, estudios previos han señalado que los regímenes de interceptación de comunicaciones en el Perú no siempre satisfacen los criterios de necesidad y proporcionalidad exigidos por los estándares internacionales[4]. En este contexto, la base legal debería entenderse como una condición necesaria, pero no suficiente, para legitimar el despliegue de sistemas de vigilancia masiva basados en IA. La implementación de estas tecnologías debería someterse, además, a un test de proporcionalidad reforzado en el que se evalúe su afectación a la libertad de expresión y a otros derechos fundamentales, acompañado de control judicial previo y mecanismos de revisión periódica sobre su necesidad y alcance.

Identificación biométrica y ausencia de protección del anonimato

El artículo 23.1.e del Decreto Supremo N.° 115-2025-PCM prohíbe el uso de sistemas de identificación biométrica en tiempo real en espacios públicos, aunque establece una serie de excepciones relevantes. Entre estas se encuentran la verificación de identidad digital y la investigación preliminar de una amplia lista de delitos graves, que incluye homicidio calificado, sicariato, feminicidio, secuestro, trata de personas, explotación sexual, robo agravado, extorsión, lavado de activos, tráfico ilícito de drogas, minería ilegal y crimen organizado, entre otros. En comparación, el AI Act contiene una prohibición prácticamente idéntica, pero que difiere en las excepciones. Bajo el régimen europeo, el uso de sistemas de identificación biométrica en tiempo real en espacios públicos está permitido únicamente para la búsqueda selectiva de personas desaparecidas o víctimas de secuestro, trata de personas o explotación sexual; la prevención de una amenaza específica, importante e inminente para la vida o la seguridad física de las personas físicas; la prevención de atentados terroristas; y para la localización o identificación de una persona sospechosa de haber cometido delitos graves con una pena máxima mayor a 4 años (terrorismo, trata de personas, explotación sexual de menores, tráfico ilícito de drogas, tráfico ilícito de armas, tráfico ilícito de órganos, tráfico ilícito de materiales nucleares o radiactivos, homicidio voluntario, secuestro, violación, sabotaje, robo organizado o a mano armada, etc.).

---

[3] Instituto de Democracia y Derechos Humanos de la PUCP (IDEHPUCP). (2023). *Vigilados en secreto: Informe expone la critica situacion de activistas y ciudadanos en entornos digitales*. https://idehpucp.pucp.edu.pe/boletin-eventos/vigilados-en-secreto-informe-expone-la-critica-situacion-de-activistas-y-ciudadanos-en-entornos-digitales/

[4] Necessary & Proportionate. (2016). *Analysis of surveillance law and practice in Peru*. https://necessaryandproportionate.org/files/peru-en-july2016.pdf

Si bien la intención declarada de la norma es restringir el uso generalizado del reconocimiento facial, la amplitud del catálogo de delitos que habilitan excepciones —sumada a la ausencia de requisitos procedimentales específicos, como la exigencia de autorización judicial previa o la supervisión independiente— genera un margen considerable para su aplicación extensiva. En la práctica, ello podría permitir justificar el uso de tecnologías de identificación biométrica en contextos como protestas o reuniones públicas, especialmente si los participantes son objeto de investigaciones relacionadas con delitos incluidos en la lista.

A ello se suma una omisión normativa significativa: el marco regulatorio peruano no reconoce explícitamente el derecho al anonimato como límite al uso de sistemas de IA. Este vacío resulta particularmente relevante, dado que el derecho a participar en la vida pública sin ser identificado constituye un componente esencial de la libertad de expresión y de reunión. Este principio ha sido reconocido tanto por el Comité de Derechos Humanos de las Naciones Unidas[5] como por la Relatoría Especial de la ONU sobre libertad de opinión y expresión[6].

Transparencia algorítmica para privados y asimetría estatal

El artículo 25 del Decreto Supremo N.° 115-2025-PCM establece que los desarrolladores o implementadores de sistemas de IA clasificados como de alto riesgo deben adoptar mecanismos que garanticen la transparencia algorítmica. Estas obligaciones incluyen informar a los usuarios sobre la finalidad del sistema, sus funcionalidades y el tipo de decisiones que puede producir, así como ofrecer mecanismos de explicabilidad de los resultados generados.

No obstante, estas obligaciones recaen principalmente sobre actores privados. El Estado —que utiliza sistemas de IA en ámbitos sensibles como la seguridad pública, la administración de programas sociales o la gestión del sistema de justicia— no se encuentra sujeto a requisitos equivalentes de transparencia. Esta asimetría normativa resulta problemática desde la perspectiva de la protección de derechos fundamentales. Los sistemas de IA utilizados por entidades públicas pueden generar impactos particularmente significativos sobre los ciudadanos, por lo que la ausencia de obligaciones de transparencia equiparables constituye una laguna regulatoria relevante.

Adicionalmente, el marco normativo no incorpora de manera explícita la libertad de expresión como límite al uso de tecnologías de IA por parte del Estado. Tampoco establece

---

[5] Organización de las Naciones Unidas (ONU). (2011). *Comentario General N. 34 del Comité de Derechos Humanos: Libertad de opinión y expresión*. CCPR/C/GC/34.

[6] Kaye, D. (2015). *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. A/HRC/29/32. Consejo de Derechos Humanos de las Naciones Unidas.

salvaguardas específicas para el uso de estas tecnologías en ámbitos vinculados al periodismo, el activismo o el discurso político. Esta omisión contrasta con el enfoque adoptado por el AI Act europeo, como se examina en la sección siguiente.

Análisis comparado: marco peruano y AI Act europeo

En la presente sección se comparará los textos de la Ley N.° 31814 y de su reglamento con el de la AI Act en ciertos aspectos clave de los marcos regulatorios establecidos. Cabe señalar que esta comparación se hace debido a que, como se mencionó previamente, los marcos regulatorios que la Unión Europea ha instaurado en materia de servicios digitales, incluso antes de la AI Act, han sido considerablemente influyentes en todo el mundo[7]. La AI Act no ha sido la excepción, y muchas de las secciones del reglamento de la ley peruana en materia de inteligencia artificial se corresponden con secciones similares en el texto europeo, lo que invita aún más a la comparación.

Esto no quiere decir que la AI Act sea la solución definitiva a la regulación de sistemas basados en inteligencia artificial, o que deba ser tomada como modelo absoluto. La legislación europea carga con sus propias deficiencias e imperfecciones. Sin embargo, la comparación de ambos textos regulatorios puede guiar una revisión crítica de la legislación peruana.

Usos prohibidos: criterios técnicos versus categorías generales

En materia de usos prohibidos, ambos marcos regulatorios convergen en la prohibición de prácticas como la manipulación de decisiones, ciertas formas de categorización biométrica y la predicción del comportamiento delictivo. Una limitación que ambos marcos regulatorios comparten, en este aspecto, es una falta de claridad en la definición de 'prácticas manipuladoras'. El reglamento europeo intenta introducir cierto grado de verificabilidad a su definición, usando términos propios de la psicología: lo que se prohíbe es el uso de técnicas subliminales que operen más allá de la conciencia de una persona con el objetivo o efecto de alterar sustancialmente el comportamiento de un individuo o grupo, mermando la capacidad de hacer una decisión informada y haciendo que tomen una decisión perjudicial que no hubieran tomado de otra forma (Comisión Europea, 2024, artículo 5). Sin embargo, esta definición aún deja vacíos en cuanto a la forma en que se podría demostrar que una práctica o funcionalidad es o no manipuladora. No queda claro en esta definición que diferencia una

[7] González, M. y Álvarez, R. (2025). Modelización regulatoria. Palpitando la influencia de la Digital Services Act en América Latina. *Latin American Journal of European Studies, 5*(1), 400-433. https://doi.org/10.51799/2763-8685v5n1017

técnica subliminal inapropiada de tácticas persuasivas permitidas; y los criterios relativos a la alteración sustancial del comportamiento, la afectación de la capacidad de decisión y la influencia en tomar una decisión "que de otro modo no habrían tomado", son subjetivos o cuando menos difícilmente comprobables.

El marco peruano, por su parte, pretende establecer una definición similar, pero que es aún menos específica. Emplea la expresión "influir de manera engañosa o manipulativa en la toma de decisiones", y específica que esto aplicaría en los casos en que se usen técnicas subliminales o el aprovechamiento de vulnerabilidades para afectar la capacidad de decisión autónoma de una persona. Esta formulación comparte problemas similares a la normativa europea, pero es incluso más amplia y potencialmente más difícil de delimitar en términos operativos.

Dejando de lado este aspecto, al ver los demás usos prohibidos en cada texto y compararlos, es importante destacar que el AI Act prohíbe prácticas que el marco peruano no regula expresamente. Entre ellas se encuentran la creación o ampliación de bases de datos de reconocimiento facial mediante la extracción no selectiva de imágenes de internet o de sistemas de videovigilancia, así como la inferencia de emociones en entornos laborales o educativos. Asimismo, el reglamento europeo prohíbe explícitamente los sistemas de IA destinados a influir en el resultado de elecciones o referendos o en el comportamiento electoral de los votantes. Estas prohibiciones no se encuentran contempladas de manera equivalente en la normativa peruana.

Libertad de expresión como límite explícito

Una diferencia particularmente relevante entre ambos marcos radica en el reconocimiento explícito de la libertad de expresión. El AI Act europeo incorpora este derecho como uno de los principios que deben guiar el diseño y la aplicación de la regulación en materia de IA. El marco peruano, en cambio, no incluye una referencia equivalente.

La ausencia de esta referencia explícita puede generar un entorno regulatorio más vulnerable a interpretaciones que no consideren adecuadamente el impacto de las tecnologías de IA sobre el discurso público, el periodismo o el activismo.

Sistemas de alto riesgo: alcance y sectores cubiertos

En relación con los sistemas de alto riesgo, ambos marcos regulatorios identifican sectores críticos como la educación, el empleo, los servicios sociales, la salud y la administración de

justicia. No obstante, el AI Act europeo desarrolla una regulación considerablemente más detallada.

El reglamento europeo incorpora listas taxativas que identifican subsectores y tipos específicos de decisiones automatizadas que deben ser considerados de alto riesgo. El marco peruano, por el contrario, utiliza categorías más amplias y menos especificadas, lo que puede generar incertidumbre respecto de qué sistemas concretos deben someterse a los requisitos regulatorios reforzados.

El panorama regulatorio en América Latina

Perú se ha posicionado como uno de los países pioneros en América Latina al contar con una ley y un reglamento específicos actualmente vigentes que establecen un marco general sobre inteligencia artificial. En la base de datos de legislación relacionada a IA del Observatorio Legislativo del Centro de Estudios en Libertad de Expresión (CELE), se puede apreciar que en todos los demás países de la región, las propuestas de marcos generales de regulación se encuentran aún en evaluación en sus respectivos congresos. Sin embargo, el análisis comparado del panorama regional revela un escenario regulatorio aún incipiente.

Argentina, por ejemplo, no cuenta con una ley nacional específica sobre IA. El Congreso mantiene en consideración múltiples proyectos legislativos —entre ellos los proyectos 2573/24, 2405/24, 2285/24, 1368/24, 3003-D-2024, 4329-D-2023 y 2505-D-2023—, pero ninguno ha sido aprobado hasta la fecha, lo que evidencia la fragmentación del debate regulatorio.

Brasil tampoco dispone de legislación vigente en la materia, aunque el proyecto de ley PL 2338/2023 ha avanzado en el Congreso y propone un esquema regulatorio basado en riesgos, con una clara influencia del modelo europeo. Chile, por su parte, ha aprobado una Política Nacional de Inteligencia Artificial y tramita actualmente el proyecto de ley Boletín 16821-19, orientado a regular los usos de estas tecnologías[8].

En otros países de la región, el debate normativo también se encuentra en desarrollo. Colombia discute el Proyecto de Ley N.° 043 de 2025 del Senado, mientras que Costa Rica cuenta con el Proyecto de Ley Expediente 23771. Ecuador tiene dos iniciativas legislativas principales en discusión (PL 450889 y PL 453516). El Salvador constituye un caso particular

[8] Ministerio de Ciencias de Chile. (2021). Política Nacional de Inteligencia Artificial. Gobierno de Chile.

al haber promulgado el Decreto N.° 234, Ley de Fomento a la Inteligencia Artificial y Tecnologías, aunque esta norma aún carece de reglamentación.

La mayoría de los países de la región cuenta con proyectos legislativos en diferentes etapas de tramitación, pero pocos han logrado consolidar marcos normativos plenamente operativos. En este contexto, el modelo peruano puede ser útil, tanto como referencia inicial como en aquellos aspectos donde sus limitaciones pueden servir de advertencia para el diseño de esquemas regulatorios en la región.

Conclusiones

Recientemente, Perú ha destacado por ser uno de los primeros países en América Latina en establecer un marco general para la regulación de sistemas basados en inteligencia artificial. Sin embargo, como se ha evidenciado, este marco presenta deficiencias, ambigüedades y vacíos preocupantes, incluso cuando se lo compara con modelos como la AI Act Europea, que tiene sus propios problemas e imperfecciones. El reglamento peruano prohíbe el uso engañoso o manipulativo de la IA, pero sin proveer definiciones claras de qué constituye tales usos; legitima la vigilancia masiva; permite el uso de sistemas de identificación biométrica en una variedad extensa de casos, sin reconocer el derecho al anonimato como límite; establece pocos y débiles controles para el Estado en el uso de sistemas basado en IA; y no reconoce la libertad de expresión como un límite necesario a tomar en cuenta en el desarrollo y uso de sistemas basados en IA.

Frente a esto, se hace necesario que que este marco regulatorio sea reevaluado a profundidad, tomando como estándar central la protección y garantía de los derechos fundamentales, especialmente la libertad de expresión, el derecho al acceso a la información y el derecho a la protección de los datos personales.