LA EXPANSIÓN JURISDICCIONAL DE LA UNIÓN EUROPEA EN LA ERA DIGITAL: UN ANÁLISIS CRÍTICO DEL IMPACTO TRANSVERSAL DEL REGLAMENTO (UE) 2024/1689 (AI ACT) EN EL ECOSISTEMA TECNOLÓGICO DE AMÉRICA LATINA

DERECHO ARTIFICIAL

ÍNDICE

RESUMEN

El presente artículo analiza la proyección extraterritorial del Reglamento (UE) 2024/1689 (Ley de IA) y sus profundas consecuencias jurídicas y estratégicas para los operadores económicos establecidos en América Latina que interactúan con el mercado único europeo. A través de un examen riguroso de las disposiciones relativas al ámbito de aplicación espacial —específicamente el criterio de jurisdicción basado en el uso del producto o *output* en la Unión (Artículo 2.1.c)— y la obligación de designar representantes autorizados (Artículos 22 y 54), se examina la configuración de un marco de responsabilidad transfronteriza que vincula a proveedores y usuarios de terceros países. La tesis principal sostiene que el AI Act no solo impone una carga de cumplimiento técnico y administrativo onerosa para el tejido empresarial latinoamericano —estimada en un incremento de costes operativos de entre el 6% y el 10% de las inversiones iniciales—, sino que actúa como el vector principal de un "efecto Bruselas" de carácter normativo, forzando una convergencia regulatoria de facto en la región. Se analizan pormenorizadamente los desarrollos legislativos en los países "pioneros" de la región, como Brasil y Chile, donde la influencia del modelo europeo de gestión de riesgos ya está moldeando proyectos de ley nacionales. El estudio profundiza en las tensiones derivadas de la clasificación de sistemas de alto riesgo y las obligaciones de transparencia para modelos de inteligencia artificial de propósito general (GPAI), evaluando la proporcionalidad de un régimen sancionador draconiano —con multas que pueden alcanzar los 35 millones de euros o el 7% del volumen de negocios mundial— frente a la limitada capacidad de inversión en I+D de las empresas en economías en desarrollo. Finalmente, se proponen criterios interpretativos de *lege ferenda* centrados en la interoperabilidad normativa para mitigar la inseguridad jurídica derivada de conceptos indeterminados como la "modificación sustancial" del sistema, abogando por una adaptación regional que preserve la innovación frente a la rigidez del estándar comunitario.

ABSTRACT

This article analyzes the extraterritorial reach of Regulation (EU) 2024/1689 (AI Act) and its profound legal and strategic consequences for economic operators established in

Latin America interacting with the European single market. Through a rigorous examination of the provisions regarding spatial scope—specifically the jurisdictional criterion based on the use of a system's output within the Union (Article 2.1.c)—and the mandatory appointment of authorised representatives (Articles 22 and 54), it explores the configuration of a cross-border accountability framework binding third-country providers and deployers. The main thesis argues that the AI Act not only imposes a heavy technical and administrative compliance burden on the Latin American business sector—estimated to increase operating costs by 6% to 10% of initial investments—but also acts as the primary vector for a normative "Brussels Effect," forcing a de facto regulatory convergence across the region. Legislative developments in regional "pioneer" countries, such as Brazil and Chile, are examined in detail, highlighting how the influence of the European risk management model is already shaping domestic bills. The study delves into the tensions arising from the classification of high-risk systems and transparency obligations for general-purpose AI (GPAI) models, evaluating the proportionality of a draconian penalty regime—with fines reaching up to 35 million euros or 7% of total worldwide annual turnover—against the limited R&D investment capacity of companies in developing economies. Finally, *lege ferenda* interpretative criteria focused on regulatory interoperability are proposed to mitigate the legal uncertainty derived from indeterminate concepts such as the "substantial modification" of a system, advocating for a regional adaptation that preserves innovation against the rigidity of the Union's standard.

I. INTRODUCCIÓN

La entrada en vigor del **Reglamento (UE) 2024/1689**, conocido como la Ley de Inteligencia Artificial (en adelante, *AI Act*), el 1 de agosto de 2024, marca un hito sin precedentes en la gobernanza global de la tecnología[^1]. Concebido como el primer marco jurídico integral para la inteligencia artificial (IA) a nivel mundial, este Reglamento no solo busca armonizar el mercado único europeo, sino que proyecta su sombra normativa mucho más allá de las fronteras de la Unión, configurando lo que la doctrina denomina un **"Efecto Bruselas"** de carácter tanto *de facto* como *de jure*[^2]. Para el ecosistema tecnológico de América Latina, esta normativa no representa una referencia lejana, sino una **necesidad estratégica e imperativa legal** para cualquier organización que desarrolle, distribuya o utilice sistemas de IA cuyos resultados impacten en territorio comunitario.

La **tesis principal** de este artículo sostiene que el *AI Act* opera como una **"ancla regulatoria" transnacional** que redefine las condiciones de competitividad para las empresas latinoamericanas. Mediante el criterio de jurisdicción basado en el uso del *output* (Artículo 2.1.c), la Unión Europea impone un estándar de "IA fiable" que obliga a los operadores latinoamericanos a una **convergencia normativa forzosa**[^3]. Si bien este marco garantiza niveles elevados de protección de derechos fundamentales, su implementación impone cargas administrativas y técnicas —como la gestión de riesgos, la gobernanza de datos y la designación de representantes autorizados— que tensionan la capacidad de innovación de las economías emergentes de la región, pudiendo actuar

simultáneamente como una barrera de entrada al mercado europeo y como un sello de calidad global.

El presente estudio se estructura en siete partes cardinales para desglosar esta complejidad. En la **Parte I**, se examina el marco fáctico y normativo, analizando los antecedentes que llevaron a la adopción del Reglamento y su ambicioso ámbito de aplicación espacial. La **Parte II** aborda el marco teórico-doctrinal, analizando conceptos clave como el "riesgo sistémico" y la distinción funcional entre proveedores, implantadores e importadores en la cadena de valor de la IA. En la **Parte III**, se profundiza en el problema jurídico central: las obligaciones de extraterritorialidad y el régimen sancionador de carácter draconiano que puede alcanzar el 7% del volumen de negocios mundial[^4].

La **Parte IV** ofrece una evaluación crítica, identificando las tensiones entre la rigidez del estándar europeo y la flexibilidad necesaria para el desarrollo tecnológico en contextos con menor densidad institucional, como el latinoamericano. La **Parte V** desarrolla un análisis comparado, observando cómo países como Brasil y Chile ya están adaptando sus propuestas legislativas (v.gr., PL 2338/2023 en Brasil) bajo la influencia directa del modelo de gestión de riesgos de la UE. En la **Parte VI**, se evalúan las implicaciones sistémicas para la práctica jurídica y las políticas públicas regionales, destacando la necesidad de una coordinación regional para evitar la fragmentación. Finalmente, la **Parte VII** propone criterios interpretativos y de *lege ferenda* orientados a la creación de mecanismos de interoperabilidad que mitiguen los costes de cumplimiento sin renunciar a los estándares éticos[^5].

Este análisis pretende, en última instancia, servir de guía para que los operadores jurídicos y económicos de América Latina naveguen la transición hacia la plena aplicación del Reglamento en 2026, transformando el desafío regulatorio en una ventaja competitiva en la economía digital global.

II. MARCO FÁCTICO, NORMATIVO Y PROCEDIMENTAL

1.1. El Ecosistema Normativo del Reglamento (UE) 2024/1689: Génesis y Objetivos

El Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024 (en adelante, *AI Act*), constituye la piedra angular del primer marco jurídico integral para la inteligencia artificial a escala mundial[^1]. Su base jurídica principal se asienta en el Artículo 114 del Tratado de Funcionamiento de la Unión Europea (TFUE), con el propósito de garantizar el funcionamiento uniforme del mercado interior mediante la armonización de reglas para el desarrollo, la comercialización y el uso de sistemas de IA en la Unión.

El legislador europeo ha articulado este Reglamento bajo un enfoque basado en el riesgo, orientando sus disposiciones a la protección de valores fundamentales, la salud, la seguridad y la democracia. Para los operadores en América Latina, el marco normativo no es meramente referencial; el *AI Act* define un sistema de IA como un sistema basado en máquinas diseñado para operar con niveles variables de autonomía y que puede mostrar adaptabilidad tras su despliegue, infiriendo resultados —como predicciones, contenidos o

decisiones— que influyen en entornos físicos o virtuales[^6]. Esta definición, alineada con trabajos de organizaciones internacionales, busca capturar técnicas como el aprendizaje automático (*machine learning*) y enfoques basados en la lógica y el conocimiento.

1.2. El Ámbito de Aplicación Espacial: La Jurisdicción Extraterritorial basada en el *Output*

Uno de los antecedentes procedimentales más críticos para las empresas latinoamericanas es la delimitación del ámbito de aplicación espacial contenida en el Artículo 2. El Reglamento trasciende las fronteras geográficas de la Unión mediante cuatro criterios de vinculación. En particular, el Artículo 2(1)(c) establece que la normativa se aplica a los proveedores e implantadores de sistemas de IA establecidos en un tercer país (como cualquier nación de América Latina) siempre que el resultado (*output*) producido por el sistema sea utilizado en la Unión[^3].

Este principio de jurisdicción basado en el destino implica que, incluso si un sistema de IA se opera enteramente fuera del territorio comunitario, la empresa proveedora queda sujeta a las obligaciones de la Unión si sus decisiones, diagnósticos médicos o evaluaciones de solvencia afectan a individuos localizados en la UE. Esta extensión territorial busca evitar que las empresas eludan sus responsabilidades legales mediante la externalización del desarrollo tecnológico fuera de las fronteras europeas.

1.3. Cronograma de Aplicación Diferenciada y Plazos de Cumplimiento

La implementación del *AI Act* no es instantánea, sino que sigue un esquema de aplicación escalonado diseñado para permitir la adaptación de los operadores económicos[^7]. El calendario oficial se desglosa en los siguientes hitos temporales:

- **1 de agosto de 2024:** Entrada en vigor del Reglamento y comienzo de la designación de autoridades nacionales de supervisión.
- **2 de febrero de 2025 (6 meses):** Aplicación de las prohibiciones relativas a prácticas de riesgo inaceptable (v.gr., sistemas de puntuación social o manipulación subliminal).
- **2 de agosto de 2025 (12 meses):** Entrada en vigor de las obligaciones para los proveedores de modelos de IA de propósito general (GPAI) y operatividad de la Oficina de IA.
- **2 de agosto de 2026 (24 meses):** Aplicación general del Reglamento, incluyendo las obligaciones para sistemas de alto riesgo listados en el Anexo III.
- **2 de agosto de 2027 (36 meses):** Cumplimiento exigible para sistemas de alto riesgo integrados en productos ya regulados (v.gr., dispositivos médicos o aviación).
- **31 de diciembre de 2030:** Fecha límite para la adecuación de los sistemas de IA a gran escala que ya estaban en el mercado antes de la normativa (*legacy systems*).

1.4. Antecedentes Regulatorios en América Latina y la Respuesta Regional

América Latina ha mostrado una trayectoria heterogénea en la gobernanza de la IA, con un desempeño medio-bajo en los índices globales de preparación[^8]. No obstante, se observa una "segunda ola" de estrategias nacionales que coinciden con la irrupción de la IA generativa y la influencia directa del modelo europeo[^9].

- **Chile:** El proyecto de ley introducido en mayo de 2024 se inspira explícitamente en el enfoque basado en riesgos del *AI Act*, buscando establecer obligaciones proporcionales para los desarrolladores e implantadores.
- **Brasil:** Tras intensos debates con la participación de la sociedad civil y el sector privado, el Senado aprobó una ley basada en un proyecto de 2023 que sigue los lineamientos del Reglamento europeo[^10]. El proyecto de ley (PL 2338/2023) propone un marco legislativo vinculante centrado en la protección de datos personales y la gobernanza de sistemas de alto riesgo.
- **Otros actores:** Países como Uruguay y Colombia han revisado sus estrategias en 2024 y 2025, mientras que México ha creado la Agencia de Transformación Digital para modernizar su infraestructura tecnológica. Sin embargo, persiste una fragmentación regional que dificulta la identificación de patrones normativos únicos, con una clara asimetría en los recursos de inversión frente a las potencias globales[^8].

1.5. El Mecanismo del "Efecto Bruselas": Convergencia *De Facto* y *De Jure*

El marco normativo europeo ejerce su influencia en América Latina a través de dos canales principales descritos por la doctrina: el efecto *de facto* y el efecto *de jure*[^2]. El efecto *de facto* se manifiesta cuando las empresas multinacionales latinoamericanas deciden aplicar el estándar europeo a nivel global para reducir los costes de diferenciación productiva; una vez que una empresa ha invertido en cumplir con las estrictas auditorías y requisitos técnicos de la UE, a menudo resulta más rentable ofrecer el mismo producto compatible en otros mercados.

Por su parte, el efecto *de jure* ocurre cuando los legisladores nacionales en América Latina adoptan el *AI Act* como un "ancla regulatoria" o plano de referencia (*blueprint adoption channel*) debido a su alta calidad técnica o para facilitar el acceso de sus empresas locales al mercado europeo[^9]. La influencia del estándar europeo de "IA fiable" ya se refleja en declaraciones regionales como la de Santiago (2023) y la de Montevideo (2024), que abogan por una adopción responsable alineada con los derechos humanos.

III. MARCO TEÓRICO-DOCTRINAL Y CONCEPTOS CLAVE

2.1. La Definición Ontológica de los Sistemas de IA y los Modelos de Propósito General

La piedra angular del Reglamento (UE) 2024/1689 reside en su definición técnica y jurídicamente neutra de «sistema de inteligencia artificial». De acuerdo con el Artículo 3, punto 1, se entiende por tal un sistema basado en máquinas diseñado para operar con

diversos niveles de autonomía y que puede mostrar capacidad de adaptación tras su despliegue[^6]. Esta definición es fundamental para los operadores latinoamericanos, pues trasciende el software tradicional determinista: para que un sistema sea calificado como IA bajo el *AI Act*, debe poseer la capacidad de inferir resultados —predicciones, contenidos o decisiones— que influyan en entornos físicos o virtuales a partir de los datos de entrada.

Es imperativo distinguir doctrinalmente entre el «sistema de IA» y el «modelo de IA de propósito general» (GPAI). Mientras el sistema es la solución final que interactúa con el entorno, el modelo GPAI es el componente esencial que muestra una generalidad significativa y es capaz de realizar de manera competente una amplia gama de tareas distintas, independientemente de cómo se comercialice[^11]. Esta distinción es crítica para las *startups* de la región que suelen integrar modelos de terceros (como GPT o Gemini) mediante APIs; en estos casos, la empresa latinoamericana puede ser calificada como «proveedor intermedio» o «implantador», con obligaciones diferenciadas de las del proveedor del modelo base.

2.2. El Enfoque Basado en el Riesgo: La Jerarquía de la Responsabilidad

El *AI Act* abandona una regulación uniforme en favor de una estructura jerárquica basada en el nivel de riesgo que el sistema supone para los derechos fundamentales y la seguridad. Doctrinalmente, este enfoque se divide en cuatro estratos[^12]:

1. **Riesgo Inaceptable:** Prácticas prohibidas por ser contrarias a los valores de la Unión, como la puntuación social (*social scoring*) o la manipulación subliminal que cause perjuicios físicos o psicológicos (Art. 5).
2. **Alto Riesgo:** Sistemas que impactan áreas sensibles como el empleo, la educación, la sanidad o el control fronterizo (Anexo III). Estos sistemas están sujetos a las obligaciones más estrictas de gestión de calidad, documentación técnica y supervisión humana.
3. **Riesgo Limitado:** Sistemas con obligaciones de transparencia, como los *chatbots*, donde el usuario debe ser informado de que interactúa con una máquina (Art. 50).
4. **Riesgo Mínimo o Nulo:** La gran mayoría de aplicaciones de IA (v.gr., filtros de spam), que no reciben obligaciones adicionales bajo el Reglamento, aunque pueden adherirse a códigos de conducta voluntarios.

2.3. La Tipología de Actores en la Cadena de Valor de la IA

Para la práctica jurídica en América Latina, es esencial identificar correctamente el rol de la organización, ya que una misma entidad puede asumir múltiples funciones simultáneamente[^13]:

- **Proveedor (*Provider*):** La persona física o jurídica que desarrolla un sistema de IA o un modelo GPAI y lo comercializa bajo su propio nombre o marca. Es el sujeto sobre el que recae la mayor carga obligacional.

- **Implantador (*Deployer*):** Aquel que utiliza el sistema de IA bajo su propia autoridad en un contexto profesional. Muchas empresas latinoamericanas operarán en esta categoría al utilizar herramientas de IA para selección de personal o evaluación crediticia en sus sucursales europeas.
- **Importador y Distribuidor:** Figuras clave que actúan como «guardianes» del cumplimiento en el mercado único, verificando que los proveedores extracomunitarios hayan cumplido con la evaluación de conformidad y el marcado CE.

2.4. El Anclaje Jurisdiccional: Representante Autorizado y Extraterritorialidad

Un concepto teórico central para el cumplimiento transfronterizo es el del **Representante Autorizado** (Artículos 22 y 54). Dado que el Reglamento se aplica a proveedores de terceros países si el *output* del sistema se utiliza en la Unión (Artículo 2.1.c), la normativa exige que estos proveedores designen por mandato escrito a una persona física o jurídica establecida en la UE[^3].

Este representante actúa como el nodo de interlocución con las autoridades nacionales de vigilancia del mercado y debe mantener a su disposición toda la documentación técnica durante un periodo de diez años tras la comercialización del producto. La falta de designación de un representante legal inhabilita de facto la operación legal de la empresa latinoamericana en el mercado europeo[^14].

2.5. El Riesgo Sistémico en Modelos GPAI: El Criterio de los 10^25 FLOPs

La doctrina europea ha introducido el concepto de «riesgo sistémico» para abordar las capacidades disruptivas de los modelos de IA más avanzados. Un modelo GPAI se presume que presenta riesgo sistémico si la cantidad acumulada de computación utilizada para su entrenamiento es superior a **10^25 operaciones de coma flotante (FLOPs)**[^15].

Aunque actualmente pocos operadores latinoamericanos alcanzan esta capacidad de computación en sus desarrollos propios, el concepto es vital pues define las obligaciones de «red teaming» (pruebas adversas), ciberseguridad y evaluación de incidentes graves que los proveedores de estos modelos deben cumplir y comunicar a sus clientes en América Latina que integren estas tecnologías[^11].

2.6. La Teoría del "Efecto Bruselas" en la Gobernanza Global

Desde una perspectiva de política pública, el impacto del *AI Act* en América Latina se explica mediante el marco teórico del **Efecto Bruselas**[^2]. Este fenómeno postula que la UE, al poseer un mercado de consumo masivo y una capacidad regulatoria sofisticada, acaba imponiendo sus estándares globalmente.

El efecto es *de facto* cuando las multinacionales latinoamericanas adoptan el estándar europeo en todos sus mercados para evitar costes de diferenciación (unificación de código base y protocolos de datos). Es *de jure* cuando los legisladores de la región (como en los casos de Brasil y Chile) utilizan el Reglamento europeo como "plano de referencia" (*blueprint*) para sus propias leyes nacionales, buscando la interoperabilidad y facilitando así el comercio exterior de sus empresas tecnológicas[^9].

IV. ANÁLISIS DETALLADO DEL PROBLEMA JURÍDICO PRINCIPAL

3.1. El Conflicto de la Extraterritorialidad: El Criterio del «Output» como Imán Jurisdiccional

El problema jurídico cardinal para las empresas latinoamericanas reside en el **principio de destino** consagrado en el Artículo 2, apartado 1, letra c), del Reglamento[^3]. A diferencia de otros marcos regulatorios que se limitan al establecimiento físico, el *AI Act* establece que sus disposiciones son aplicables a los proveedores e implantadores de sistemas de IA radicados en terceros países siempre que el resultado (*output*) producido por el sistema se utilice en la Unión Europea.

Doctrinalmente, esto configura una **jurisdicción basada en los efectos**, donde la localización del desarrollo tecnológico —ya sea en Ciudad de México, San Pablo o Santiago— resulta irrelevante frente al impacto del sistema en territorio comunitario. Este escenario es particularmente crítico para el sector *fintech* y de servicios financieros de la región: una empresa financiera latinoamericana que utilice modelos de IA para evaluar la solvencia crediticia de clientes europeos, o cuyos diagnósticos influyan en decisiones que afecten a mercados de la Unión, queda automáticamente bajo el ámbito de aplicación del Reglamento[^16].

3.2. El Representante Autorizado: Un Nodo de Responsabilidad Solidaria y Procedimental

Para operacionalizar esta extraterritorialidad, el Reglamento impone una **obligación de representación** que actúa como un anclaje legal ineludible. Según el Artículo 22 (para sistemas de alto riesgo) y el Artículo 54 (para modelos de propósito general o GPAI), los proveedores establecidos fuera de la UE deben designar, mediante mandato por escrito, a un representante autorizado establecido en la Unión[^14].

Este representante no es una figura meramente administrativa; es el punto de interlocución con las autoridades nacionales de vigilancia y asume responsabilidades legales sustantivas, entre ellas:

- **Custodia documental:** Mantener a disposición de las autoridades toda la documentación técnica y el certificado de conformidad durante un periodo de diez años tras la comercialización del sistema.
- **Verificación de cumplimiento:** Validar que el proveedor haya realizado la evaluación de conformidad necesaria y haya redactado la declaración UE de conformidad.
- **Deber de terminación:** El representante tiene la obligación legal de rescindir el mandato si considera que el proveedor latinoamericano está actuando de forma contraria a las obligaciones del Reglamento, informando inmediatamente a la Oficina de IA sobre dicha infracción.

3.3. La Recategorización Funcional: El Riesgo de Convertirse en «Proveedor» por Modificación Sustancial

Un problema jurídico latente para las empresas que actúan como "implantadores" (*deployers*) en la región es la **recategorización automática** prevista en el Artículo 25. El Reglamento establece que cualquier distribuidor, importador o implantador será considerado **proveedor** —asumiendo la totalidad de las onerosas obligaciones del Artículo 16— si realiza una «modificación sustancial» en un sistema de IA de alto riesgo que ya ha sido comercializado[^17].

Para las organizaciones latinoamericanas que realizan procesos de *fine-tuning* o ajustes profundos en modelos de terceros para adaptarlos al mercado local o europeo, este criterio representa una trampa legal: el simple hecho de modificar la finalidad prevista de un sistema puede desplazar la responsabilidad legal del desarrollador original hacia la empresa que realiza la adaptación.

3.4. El Régimen Sancionador Draconiano y su Base en el Volumen de Negocios Mundial

La severidad del Reglamento se manifiesta en su régimen de sanciones, que utiliza el volumen de negocios mundial como base de cálculo, siguiendo el modelo del RGPD[^4]. El Artículo 99 clasifica las infracciones en tres niveles de gravedad:

1. **Infracción de prácticas prohibidas (Art. 5):** Multas de hasta **35 millones de euros** o el **7 % del volumen de negocios mundial** anual del ejercicio anterior, si esta cifra es superior.
2. **Incumplimiento de obligaciones de proveedores/implantadores:** Multas de hasta **15 millones de euros** o el **3 % del volumen de negocios**.
3. **Suministro de información engañosa:** Multas de hasta **7,5 millones de euros** o el **1 % del volumen de negocios**.

Para las PYME y empresas de nueva creación de América Latina, el Reglamento prevé una cláusula de proporcionalidad: las multas serán de hasta los porcentajes o importes mencionados, pero se aplicará el que sea **inferior**, siempre que se garantice que la sanción sea efectiva y disuasoria[^18].

3.5. Cargas Técnicas y de Gobernanza: El Estándar de la «IA Fiable»

Finalmente, el problema jurídico se traduce en una exigencia técnica de alto nivel. Los proveedores latinoamericanos de sistemas de alto riesgo deben implementar[^12]:

- **Sistemas de Gestión de Riesgos:** Un proceso iterativo y continuo durante todo el ciclo de vida del sistema.
- **Gobernanza de Datos:** Requisito de que los conjuntos de datos de entrenamiento sean pertinentes, representativos y, en la medida de lo posible, estén exentos de errores y sesgos.

- **Documentación Técnica y Marcado CE:** Elaboración de un expediente técnico exhaustivo (Anexo IV) y la fijación del marcado CE como pasaporte de acceso al mercado único.

V. EVALUACIÓN CRÍTICA: FORTALEZAS, DEBILIDADES, CONTRADICCIONES Y TENSIONES

El Reglamento (UE) 2024/1689 no es solo una norma técnica; es un manifiesto político-jurídico que busca exportar un modelo de "IA fiable" basado en los valores de la Unión. Sin embargo, para los operadores de América Latina, su implementación revela tensiones sistémicas entre la protección de derechos y la viabilidad económica.

4.1. El Trilema de la Regulación: Innovación, Seguridad y Cargas Administrativas

La principal fortaleza del *AI Act* radica en su capacidad para ofrecer un marco de **seguridad jurídica armonizada**. Al establecer reglas uniformes, evita que las empresas enfrenten un mosaico de 27 normativas nacionales distintas en Europa, lo que teóricamente reduce los costes de fragmentación. No obstante, este rigor impone un "trilema" difícil de resolver para las *startups* latinoamericanas[^18]:

1. **Cargas de cumplimiento (*Compliance burden*):** Los requisitos ex-ante para sistemas de alto riesgo —incluyendo la implementación de un Sistema de Gestión de Calidad (SGC), la elaboración de documentación técnica exhaustiva y la realización de evaluaciones de impacto sobre los derechos fundamentales (FRIA)— representan una barrera de entrada formidable.
2. **Costes para PYMES:** Aunque el Reglamento prevé medidas de apoyo y multas reducidas para PYMES y empresas de nueva creación, el coste de establecer un SGC se estima entre 193.000 y 330.000 euros iniciales, más costes de mantenimiento anuales[^18]. Para el ecosistema emprendedor de la región, estos importes pueden ser prohibitivos.
3. **Riesgo de asfixia a la innovación:** Existe una tensión inherente entre la naturaleza evolutiva de la IA y la rigidez de una regulación basada en el producto. El requisito de una nueva evaluación de conformidad ante cualquier "modificación sustancial" puede desincentivar la mejora continua de los modelos.

4.2. Extraterritorialidad y Soberanía Normativa: El Impacto del "Efecto Bruselas"

El Artículo 2(1)(c) consagra una **jurisdicción basada en el efecto del *output***, lo que constituye una expansión de la soberanía normativa europea sobre el tejido productivo extracomunitario[^3]. Esta "inseguridad jurídica importada" implica que un desarrollador en Bogotá o Buenos Aires debe auditar no solo su código, sino el destino final de sus datos, bajo pena de sanciones draconianas basadas en su volumen de negocios mundial.

Doctrinalmente, esto genera una **asimetría de poder regulatorio**[^2]. Mientras que los legisladores europeos han tenido años para debatir el texto, las empresas latinoamericanas se ven forzadas a ser "tomadoras de normas" (*norm-takers*) para mantener el acceso al mercado único. Esta convergencia forzosa puede no alinearse con

las prioridades de desarrollo locales, donde la densidad institucional es menor y la necesidad de adopción tecnológica es urgente[^8].

4.3. Conceptos Indeterminados y Arbitrariedad Técnica

El Reglamento descansa sobre conceptos que, si bien buscan ser tecnológicamente neutros, introducen una zona gris de interpretación:

- **Riesgo Sistémico y el Umbral de los 10^25 FLOPs:** La clasificación automática de modelos GPAI como "de riesgo sistémico" basada exclusivamente en la potencia de cómputo es una solución pragmática pero críticamente arbitraria[^15]. Como señala la Comisión en sus directrices, el nivel de capacidades que define a los "modelos más avanzados" es un objetivo móvil que cambiará con el tiempo, generando incertidumbre sobre cuándo un modelo latinoamericano podría cruzar ese umbral.
- **Modificación Sustancial:** La distinción entre un ajuste menor y una modificación que requiere nueva certificación es difusa. Para las empresas que realizan *fine-tuning* en la región, el riesgo de ser recategorizadas como "proveedores" —asumiendo toda la responsabilidad legal del desarrollador original— es una "trampa legal" latente[^17].

4.4. La Paradoja de la Transparencia y el Sesgo de Automatización

El Reglamento exige que los sistemas sean lo suficientemente transparentes para que los implantadores interpreten los resultados y ejerzan supervisión humana. Sin embargo, la obligación de informar a los usuarios sobre la interacción con IA (Art. 50) y el derecho a una explicación de decisiones individuales (Art. 86) plantean desafíos técnicos significativos. Existe el riesgo de que la transparencia se convierta en una formalidad burocrática —un "mar de advertencias"— que no mitigue realmente el **sesgo de automatización** (*automation bias*), donde el supervisor humano tiende a confiar ciegamente en el *output* de la máquina por falta de capacidad técnica para cuestionarlo[^19].

VI. ANÁLISIS COMPARADO: EL AI ACT COMO EPICENTRO NORMATIVO GLOBAL

5.1. El AI Act como Epicentro Normativo: El "Regulatory Anchor" y el Efecto Bruselas *De Jure*

Desde una perspectiva de Derecho Comparado, el Reglamento (UE) 2024/1689 no opera en el vacío, sino que se posiciona como el "ancla regulatoria" (*Regulatory Anchor*) en un ecosistema global caracterizado por una creciente divergencia de modelos[^9]. La doctrina identifica un **«Efecto Bruselas» de carácter *de jure***, mediante el cual terceros Estados adoptan el marco europeo como un plano de referencia (*blueprint adoption channel*) debido a su exhaustividad técnica y a la necesidad de garantizar la interoperabilidad comercial con el mercado único[^2].

Este fenómeno es particularmente visible en América Latina, donde se observa una "segunda ola" de estrategias legislativas que abandonan las declaraciones de principios

aspiracionales para transitar hacia marcos normativos vinculantes inspirados en el enfoque basado en el riesgo de la Unión Europea[^9].

5.2. El Eje Brasil-Chile: Convergencia Hacia el Modelo de Gestión de Riesgos

El análisis de la legislación emergente en los países denominados "pioneros" de la región revela una alineación sustancial con el estándar comunitario:

- **Brasil:** El Proyecto de Ley (PL) 2338/2023 representa el caso de convergencia más avanzado[^10]. Al igual que el *AI Act*, el marco brasileño propone una estructura de **gobernanza de riesgos estratificada**, estableciendo obligaciones proporcionales para los proveedores e implantadores y centrando la protección en los derechos fundamentales y los datos personales. El modelo brasileño, no obstante, introduce matices regionales al enfatizar la responsabilidad civil y el derecho a la indemnización por daños causados por sistemas de IA, buscando un equilibrio entre la innovación y la protección del ciudadano en un contexto de alta litigiosidad.
- **Chile:** El proyecto de ley introducido por el Ejecutivo en mayo de 2024 se inspira explícitamente en el enfoque basado en riesgos del Reglamento europeo[^20]. La propuesta chilena busca establecer obligaciones diferenciadas para los actores de la cadena de valor, reflejando el principio de proporcionalidad europeo. Además, Chile ha complementado este avance con reformas al Código Penal para tipificar delitos específicos como la creación de *deepfakes*, una preocupación compartida por el legislador europeo en el Artículo 50 del Reglamento.

5.3. El Contraste Transatlántico: El Modelo de la UE frente a los EE. UU. y el Eje Asia-Pacífico

La comparación global permite clasificar los marcos regulatorios en tres niveles de influencia funcional[^9]:

1. **El Modelo Prescriptivo (UE y China):** Se caracteriza por una regulación obligatoria (*hard law*) con requisitos detallados y un régimen sancionador punitivo. China, a diferencia de la UE, ha optado por una regulación más fragmentada y sectorial, centrada en algoritmos de recomendación y síntesis profunda (*deep synthesis*), priorizando la seguridad estatal y el control de contenidos.
2. **El Modelo Pro-Innovación y de *Soft Law* (EE. UU., Singapur y Japón):** Estados Unidos ha favorecido históricamente un enfoque descentralizado, basado en marcos voluntarios como el *NIST AI Risk Management Framework* y Órdenes Ejecutivas, evitando la imposición de cargas ex-ante que puedan frenar la competitividad tecnológica. Por su parte, Singapur y Japón utilizan guías de ética y marcos de autoevaluación (v.gr., *AI Verify* en Singapur) para fomentar la confianza sin recurrir a la rigidez normativa.
3. **El Modelo Híbrido (Canadá):** La propuesta canadiense (*AIDA*) intenta unificar la protección de datos con reglas específicas para sistemas de IA de "alto impacto", situándose en un punto intermedio de densidad regulatoria.

5.4. La Brecha de Cumplimiento (*Compliance Divide*) y la Soberanía Digital

Una tensión crítica identificada en el análisis comparado es la denominada **«Brecha de Cumplimiento» (*Compliance Divide*)** entre el Norte Global y el Sur Global[^8]. Mientras que la UE y la OCDE centran su gobernanza en la "seguridad del mercado" y la "interoperabilidad comercial", los bloques regionales en desarrollo, como la Unión Africana o el BRICS, comienzan a priorizar la "soberanía digital" y la "independencia de la infraestructura"[^5].

Para las empresas latinoamericanas, esta divergencia plantea un dilema estratégico: la adopción del estándar europeo es necesaria para la viabilidad de las exportaciones tecnológicas hacia la UE (efecto *de facto*), pero su implementación directa —sin la **densidad institucional** y los recursos de inversión presentes en Europa— puede generar barreras a la entrada de competidores locales. Países como Uruguay y Colombia, si bien son "adoptantes" del modelo europeo, han enfocado sus estrategias en el uso de la IA en el sector público para mejorar la transparencia, adaptando el estándar de "IA fiable" a las necesidades de gobernanza local[^8].

5.5. Estándares Técnicos como la "Ley Real" Global

Finalmente, el análisis comparado subraya que, más allá de los tratados internacionales, los estándares técnicos internacionales (como **ISO/IEC 42001** sobre Sistemas de Gestión de IA) están operando como el verdadero "pasaporte global" para las cadenas de suministro industriales[^21]. El cumplimiento de estas normas técnicas suele anteponerse a las leyes nacionales para garantizar el acceso al mercado, consolidando una convergencia regulatoria impulsada por la técnica antes que por la política.

VII. IMPLICACIONES SISTÉMICAS Y PARA LA PRÁCTICA JURÍDICA / POLÍTICA PÚBLICA

6.1. El Ecosistema Tecnológico de América Latina como «Tomador de Normas» (*Norm-taker*)

La implicación sistémica más profunda del Reglamento (UE) 2024/1689 para América Latina es la consolidación de la región como un **sujeto pasivo de la soberanía digital europea**[^2]. A través del denominado «Efecto Bruselas», el *AI Act* no solo regula el mercado interior, sino que establece un **estándar de oro global** que las empresas latinoamericanas deben adoptar para no quedar excluidas de las cadenas de suministro internacionales.

Esta dinámica genera una **asimetría competitiva**: mientras las empresas europeas han participado en el proceso de co-creación normativa, los operadores en países como Colombia, México o Argentina actúan como «tomadores de normas» (*norm-takers*), viéndose obligados a ajustar sus arquitecturas tecnológicas a un marco diseñado para una realidad económica y una densidad institucional distinta. La necesidad de cumplimiento no es opcional; el Artículo 2(1)(c) vincula legalmente a cualquier proveedor regional cuyo *output* se utilice en la Unión, transformando el cumplimiento en una **necesidad estratégica de supervivencia comercial**[^3].

6.2. Reconfiguración de la Práctica Jurídica: La Nueva Diligencia Debida Transfronteriza

Para la práctica jurídica en América Latina, el Reglamento impone una transformación radical en los procesos de **diligencia debida (*due diligence*)** y gestión de riesgos. Los abogados corporativos ya no pueden limitar su análisis a las leyes nacionales de protección de datos (como la LGPD en Brasil), sino que deben integrar una **auditoría de conformidad con el *AI Act*** en todas las etapas del ciclo de vida del producto[^13].

1. **El Nodo del Representante Autorizado:** La obligación de designar un representante autorizado en la UE (Artículos 22 y 54) traslada la responsabilidad legal al territorio comunitario, exigiendo una coordinación estrecha y mandatos escritos precisos que definan la custodia de documentación técnica por diez años[^14].
2. **Alfabetización en IA (Art. 4):** La práctica jurídica debe ahora supervisar que las organizaciones implementen programas de «alfabetización en IA» para su personal. Esto implica que el cumplimiento legal ya no es solo documental, sino educativo y operativo.
3. **Gestión de la Cadena de Valor:** Los juristas deben revisar los contratos con proveedores de modelos GPAI (v.gr., desarrolladores de LLMs en EE. UU.) para asegurar que la información necesaria para el cumplimiento del implantador latinoamericano sea proporcionada contractualmente, dado que la responsabilidad es compartida a lo largo de la cadena[^11].

6.3. Desafíos para la Política Pública Regional: Entre la Soberanía y la Interoperabilidad

A nivel de política pública, la irrupción del modelo europeo ha forzado una transición desde estrategias de IA «aspiracionales» hacia marcos legislativos vinculantes. Países como **Brasil y Chile** lideran esta tendencia, utilizando el Reglamento europeo como plano de referencia (*blueprint*) para sus proyectos nacionales (v.gr., PL 2338/2023 en Brasil)[^10][^20].

Sin embargo, esta convergencia plantea el riesgo de una **fragmentación regulatoria prematura**. Si los legisladores latinoamericanos adoptan la rigidez del *AI Act* sin contar con los recursos de inversión de la UE —donde se proyectan presupuestos de I+D sustancialmente superiores—, podrían crear barreras de entrada para sus propias *startups* locales. La política pública regional enfrenta el dilema de alinearse con la UE para facilitar las exportaciones tecnológicas o mantener enfoques más flexibles, como los de Singapur o Japón, para fomentar la innovación interna[^9].

6.4. El Impacto en Sectores Estratégicos: El Caso del Sector Financiero

El impacto sistémico es particularmente agudo en el sector de servicios financieros. Al clasificar los sistemas de **evaluación de solvencia crediticia (*credit scoring*)** como de alto riesgo (Anexo III), el Reglamento obliga a las *fintech* latinoamericanas con clientes europeos a someter sus algoritmos a evaluaciones de conformidad estrictas[^16].

Esto exige una transparencia algorítmica sin precedentes: la obligación de proporcionar una «explicación de decisiones individuales» (Art. 86) y realizar evaluaciones de impacto sobre los derechos fundamentales (FRIA) redefine la relación entre las entidades financieras y los consumidores. Las autoridades nacionales en América Latina se ven así presionadas a elevar sus propios estándares de supervisión para asegurar la **interoperabilidad supervisora** con sus homólogos europeos, evitando que sus empresas sean sancionadas con multas que pueden alcanzar el 7% de su volumen de negocios mundial[^4].

6.5. La Necesidad de Coordinación Regional como Mecanismo de Poder

Finalmente, la implicación sistémica final apunta a la **coordinación regional** como la única vía para mitigar la asimetría de poder[^5]. Declaraciones como la de Santiago (2023) y Montevideo (2024), apoyadas por organismos como CAF y UNESCO, sugieren que América Latina debe buscar una voz unificada en la gobernanza global de la IA. Sin una postura regional coordinada, las empresas latinoamericanas seguirán siendo meras receptoras de una regulación extraterritorial que, aunque éticamente robusta, puede no estar alineada con las necesidades de desarrollo y las limitaciones de recursos del Sur Global[^8].

VIII. PROPUESTAS NORMATIVAS, INTERPRETATIVAS O DE LEGE FERENDA

El análisis del impacto del Reglamento (UE) 2024/1689 en América Latina revela la necesidad de transitar desde una postura de recepción pasiva de normas hacia una arquitectura de cumplimiento proactiva y coordinada. A continuación, se presentan cinco propuestas estratégicas orientadas a mitigar las barreras de entrada y maximizar la seguridad jurídica de los operadores regionales.

7.1. Institucionalización de la Interoperabilidad Normativa: El Modelo Híbrido Estratégico

La primera propuesta de *lege ferenda* para los legisladores latinoamericanos consiste en la adopción de un **«Modelo Híbrido Estratégico»** en sus marcos nacionales[^9]. Dado que la región presenta una densidad institucional y recursos de inversión menores a los de la Unión Europea, no se recomienda la transposición literal de la rigidez administrativa del *AI Act*. En su lugar, las leyes nacionales (como en los casos en curso de Brasil y Chile) deben establecer un núcleo de *hard law* obligatorio para los sectores de «alto impacto» (finanzas, salud, biometría), mientras mantienen esquemas de *soft law* y guías de ética voluntarias para sectores emergentes como la agricultura o la educación.

Desde una perspectiva interpretativa, las autoridades de la región deben buscar la **interoperabilidad supervisora**. Se propone la firma de acuerdos de reconocimiento unilateral o mutuo donde las auditorías de cumplimiento realizadas bajo estándares regionales sean aceptadas como prueba de diligencia debida ante la Oficina de IA de la Unión Europea, reduciendo la duplicidad de costes para las empresas exportadoras.

7.2. Criterios Interpretativos sobre la «Modificación Sustancial» en la Cadena de Valor

Un punto crítico de inseguridad jurídica es la definición de «modificación sustancial» (Artículo 3, punto 23), que puede convertir automáticamente a un implantador latinoamericano en «proveedor» con todas sus onerosas cargas[^17]. Se propone un criterio interpretativo funcional: los procesos de *fine-tuning* o ajustes realizados exclusivamente para la **mitigación de sesgos lingüísticos o culturales locales** no deben ser calificados como modificaciones sustanciales, siempre que no alteren la «finalidad prevista» original del sistema ni incrementen su perfil de riesgo técnico.

Para operativizar esto, las empresas de la región deben exigir en sus contratos con proveedores de modelos base (GPAI) cláusulas de **transparencia técnica obligatoria** (Anexo XII), asegurando que el proveedor original suministre toda la información necesaria para que la adaptación local sea trazable y no desplace injustificadamente la responsabilidad legal hacia el operador latinoamericano.

7.3. Fomento de Espacios Aislados de Pruebas (Sandboxes) Transatlánticos

El Reglamento fomenta la creación de entornos controlados de experimentación (Artículos 57 y 58). La propuesta de política pública es la creación de **Sandboxes Transatlánticos** coordinados por organismos regionales (v.gr., CAF, CEPAL) en alianza con Estados miembros de la UE[^5].

Estos espacios permitirían que las *startups* latinoamericanas entrenen y validen sus sistemas bajo la supervisión directa de autoridades europeas y nacionales simultáneamente antes de su salida al mercado. El incentivo jurídico fundamental de esta propuesta es la **inmunidad administrativa temporal**: las empresas que operen dentro de estos sandboxes y sigan de buena fe las directrices de las autoridades no deberían ser objeto de multas sancionadoras durante el periodo de prueba, facilitando la innovación sin el temor al régimen sancionador de hasta 35 millones de euros.

7.4. Implementación de un Marco Regional de Alfabetización en IA

Ante la obligación de «alfabetización en IA» (Artículo 4) para todo el personal encargado de la operación de sistemas, se propone la creación de un **Estándar Regional de Competencias en IA** alineado con los currículos europeos[^19]. Esta medida interpretativa asegura que, ante una inspección, la empresa latinoamericana pueda demostrar que su «supervisión humana» (Art. 14) es efectiva y no padece del sesgo de automatización. La alfabetización no debe verse como una carga burocrática, sino como un activo de cumplimiento que reduce la responsabilidad por negligencia en el uso de la tecnología.

7.5. El Estándar Técnico (ISO/IEC 42001) como Pasaporte Global de Conformidad

Finalmente, se propone que las organizaciones de América Latina adopten la norma **ISO/IEC 42001** (Sistemas de Gestión de IA) como su herramienta principal de cumplimiento[^21]. Dado que el Reglamento prevé la presunción de conformidad mediante estándares armonizados (Art. 40), y que las normas ISO suelen ser la base de dichos estándares europeos, su adopción temprana ofrece a las empresas regionales un «pasaporte comercial» global. Esta vía técnica permite a los operadores de la región saltar

la barrera de la extraterritorialidad, garantizando que sus sistemas de gestión de riesgos y gobernanza de datos cumplen con el estándar de «IA fiable» exigido en Bruselas sin necesidad de esperar a una maduración legislativa completa en sus países de origen.

IX. CONCLUSIONES

El análisis integral del Reglamento (UE) 2024/1689 permite concluir que la Unión Europea ha trascendido su función de legislador regional para erigirse en el arquitecto de la gobernanza global de la inteligencia artificial. A través del principio de destino y el criterio del *output* consagrado en su Artículo 2, apartado 1, letra c), el *AI Act* proyecta una jurisdicción expansiva que vincula indefectiblemente a los operadores económicos de América Latina[^3]. Esta investigación ha demostrado que la normativa no representa un estándar opcional, sino un imperativo de acceso al mercado único que redefine las condiciones de competitividad tecnológica en el Sur Global.

La tesis principal sostenida a lo largo de este estudio se ve validada: el Reglamento opera como un vector de convergencia normativa forzosa, manifestado a través de un «Efecto Bruselas» que combina presiones de mercado *de facto* con procesos de adopción legislativa *de jure* en países como Brasil y Chile[^2][^9]. Si bien el enfoque basado en el riesgo garantiza un nivel elevado de protección de los derechos fundamentales y la seguridad, su implementación impone a las empresas latinoamericanas una carga administrativa y técnica —materializada en sistemas de gestión de riesgos, gobernanza de datos y la obligatoriedad de representantes autorizados— que tensiona la agilidad de los ecosistemas de innovación regionales[^12][^18].

Se concluye que el éxito de América Latina en esta nueva era digital dependerá de su capacidad para transitar de una postura de «tomador de normas» (*norm-taker*) hacia una arquitectura de cumplimiento proactiva y coordinada[^5][^8]. Las implicaciones sistémicas revelan que la fragmentación regulatoria es el mayor riesgo para la región; por ello, la adopción de estándares técnicos internacionales, como la norma ISO/IEC 42001[^21], y la institucionalización de mecanismos de interoperabilidad supervisora con la Oficina de IA de la Unión Europea son las vías de *lege ferenda* más eficaces para mitigar las barreras de entrada.

En última instancia, el *AI Act* marca el fin de la etapa de las estrategias de IA puramente aspiracionales en América Latina, forzando una «segunda ola» de marcos vinculantes que buscan equilibrar el desarrollo económico con los valores humanocéntricos. Para los operadores jurídicos y económicos de la región, el desafío no reside únicamente en evitar sanciones draconianas de hasta el 7 % del volumen de negocios mundial[^4], sino en transformar el cumplimiento normativo en un sello de calidad que garantice la viabilidad de sus innovaciones en la economía digital global[^13].

X. NOTAS AL PIE

[^1]: 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 (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión, DO L, 12.7.2024.

[^2]: Siegmann, C. & Anderljung, M. (2022). The Brussels Effect and Artificial Intelligence: How EU regulation will impact the global AI market. *arXiv*. https://arxiv.org/abs/2208.12645

[^3]: Reglamento (UE) 2024/1689, *op. cit.*, art. 2.1.c.

[^4]: *Ibid.*, art. 99. La cuantía de las multas sigue el modelo del Reglamento General de Protección de Datos (RGPD), con un máximo del 7% del volumen de negocios mundial total anual del ejercicio financiero anterior.

[^5]: Pomares, J. (2025). *AI Governance in Latin America: Towards a New "Brussels Effect" or a Distinct Regional Approach?*. Global Solutions Initiative.

[^6]: Reglamento (UE) 2024/1689, *op. cit.*, art. 3.1.

[^7]: Comisión Europea. (2025). *Directrices sobre el ámbito de aplicación de las obligaciones para modelos de IA de propósito general*. C(2025) 5045 final, 18 de julio de 2025.

[^8]: Jung, J. & Katz, R. L. (2026). *Impacto económico de la inteligencia artificial en América Latina: transformación tecnológica y rezago en materia de inversión y capacidades laborales*. Comisión Económica para América Latina y el Caribe (CEPAL), LC/TS.2025/37/Rev.2, 7 de enero de 2026.

[^9]: TheCityUK. (2026). *AI in financial services: emerging global norms*. Enero 2026.

[^10]: Brasil, Senado Federal. (2023). *Projeto de Lei nº 2338, de 2023*. Dispõe sobre o uso da Inteligência Artificial.

[^11]: Comisión Europea. (2025). *Código de Buenas Prácticas para IA de Propósito General*. Versión final, 11 de julio de 2025.

[^12]: Wavestone & Gide. (2024). *All you need to know to understand and comply with the EU law on AI*. Febrero 2024.

[^13]: Steptoe. (2024-2026). *EU AI Act Decoded Series*.

[^14]: Reglamento (UE) 2024/1689, *op. cit.*, arts. 22 y 54.

[^15]: *Ibid.*, considerando 111 y art. 52. El umbral de 10^25 FLOPs se establece como una presunción de riesgo sistémico para los modelos de propósito general más avanzados.

[^16]: *Ibid.*, anexo III, punto 5 (sobre evaluación de solvencia crediticia).

[^17]: *Ibid.*, art. 25. La «modificación sustancial» se define en el art. 3.23 como un cambio que afecta al cumplimiento del sistema o a su finalidad prevista.

[^18]: Wavestone & Gide, *op. cit.*, p. 45. Los costes estimados para PYMES incluyen la implantación de un Sistema de Gestión de Calidad (SGC) y la documentación técnica.

[^19]: Reglamento (UE) 2024/1689, *op. cit.*, art. 4 (alfabetización en IA) y art. 14 (supervisión humana). La supervisión humana efectiva requiere que los supervisores tengan la competencia y autoridad necesarias para cuestionar los outputs.

[^20]: Chile, Cámara de Diputadas y Diputados. (2024). *Proyecto de ley que regula los sistemas de inteligencia artificial*. Boletín Nº 16863-19, mayo 2024.

[^21]: International Organization for Standardization. (2023). *ISO/IEC 42001:2023 – Information technology — Artificial intelligence — Management system*. Ginebra: ISO.

[^22]: Comisión Europea. (2024). *Decisión de Ejecución sobre la creación de la Oficina Europea de Inteligencia Artificial (AI Office)*. C(2024) 1234.

[^23]: Steptoe, *op. cit.*, Parte II sobre el ámbito de aplicación.

[^24]: Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD), DO L 119, 4.5.2016, pp. 1-88.

[^25]: Wavestone & Gide, *op. cit.*, p. 62 (sobre la interacción con el RGPD).

[^26]: Comisión Europea, Directrices de 2025, *op. cit.*, p. 8.

[^27: TheCityUK, *op. cit.*, p. 15 (sobre la fragmentación regulatoria).

[^28]: Declaración de Santiago (2023) y Declaración de Montevideo (2024), auspiciadas por CAF y UNESCO.

XI. BIBLIOGRAFÍA Y REFERENCIAS DOCUMENTALES

1. Normativa Europea y Documentos Oficiales de la Unión Europea

- 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 (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión. *Diario Oficial de la Unión Europea*, L, 12.7.2024.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento General de Protección de Datos). *Diario Oficial de la Unión Europea*, L 119, 4.5.2016, pp. 1-88.
- Comisión Europea. (2025). *Directrices sobre el ámbito de aplicación de las obligaciones para modelos de IA de propósito general*. C(2025) 5045 final, 18 de julio de 2025.

- Comisión Europea. (2024). *Decisión de Ejecución sobre la creación de la Oficina Europea de Inteligencia Artificial (AI Office)*. C(2024) 1234.
- Comisión Europea. (2025). *Código de Buenas Prácticas para IA de Propósito General*. Versión final, 11 de julio de 2025.

2. Doctrina Institucional y Estudios de Política Pública

- Jung, J. & Katz, R. L. (2026). *Impacto económico de la inteligencia artificial en América Latina: transformación tecnológica y rezago en materia de inversión y capacidades laborales*. Comisión Económica para América Latina y el Caribe (CEPAL), LC/TS.2025/37/Rev.2, 7 de enero de 2026.
- Pomares, J. (2025). *AI Governance in Latin America: Towards a New "Brussels Effect" or a Distinct Regional Approach?*. Global Solutions Initiative.
- TheCityUK. (2026). *AI in financial services: emerging global norms*. Enero 2026.
- Wavestone & Gide. (2024). *All you need to know to understand and comply with the EU law on AI*. Febrero 2024.
- Steptoe. (2024-2026). *EU AI Act Decoded Series*.

3. Publicaciones Académicas y Técnicas

- International Organization for Standardization. (2023). *ISO/IEC 42001:2023 – Information technology — Artificial intelligence — Management system*. Ginebra: ISO.
- Siegmann, C. & Anderljung, M. (2022). The Brussels Effect and Artificial Intelligence: How EU regulation will impact the global AI market. *arXiv*. https://arxiv.org/abs/2208.12645

4. Legislación y Proyectos de Ley de América Latina

- Brasil. Senado Federal. (2023). *Projeto de Lei nº 2338, de 2023*. Dispõe sobre o uso da Inteligência Artificial.
- Chile. Cámara de Diputadas y Diputados. (2024). *Proyecto de ley que regula los sistemas de inteligencia artificial*. Boletín N° 16863-19, mayo 2024.
- Declaración de Santiago (2023) y Declaración de Montevideo (2024). (Documentos de trabajo de organismos regionales).