

Protección de la soberanía: un marco empírico de vulnerabilidad y un escudo regulatorio para la IA en una potencia media

Max Pinelo · Pilar Moncada

Junio 2026

With Apart Research

Track 1: Latin America · Subtrack: AI Governance

Plataforma VIGÍA (acceso temporal): <https://vigia-2-0-dndcq6pipa-uc.a.run.app/es/>

Resumen

Las potencias medias no pueden **construir**, **disuadir** (MAD) ni **sabotear** (MAIM) la IA de frontera, ya que las doctrinas de seguridad vigentes suponen una paridad que no tienen. Pero conservan una capacidad que la dependencia no les quita: la de **ponerse sus propias reglas y verificar y auditar que se cumplan**. Sobre ella proponemos un marco general y reproducible que le da a un gobierno dos cosas concretas. **(1) Un diagnóstico, VIGÍA¹**, observatorio que lee íntegros dos niveles, el normativo (el diario oficial) y el fáctico (la prensa), sobre quince categorías de riesgo, y mide con números el alto riesgo que el Estado opera sin ley que la regule ni auditoría, y de quién depende. **(2) Una propuesta de prevención y mitigación derivada de ese diagnóstico, SARA**, un escudo de **cinco leyes**, una por cada forma en que la dependencia puede usarse como arma de presión, cada una de las cuales previene y mitiga ese uso, sin pretender eliminar la dependencia, sino buscando volverla **no-armable**. El resultado es una **agenda legislativa accionable**: qué ley conviene aprobar primero y por qué. Este artículo presenta en detalle la **primera capa, ya operativa, VIGÍA**, y muestra cómo el escudo de leyes se deriva de lo que mide. México (2025–2026) es el caso de estudio, no el límite: 153 ediciones del Diario Oficial (665 hallazgos, 1 466 etiquetas de riesgo) y 4 327 notas de prensa muestran 95,6 % de vacío regulatorio, 82 % de “IA silenciosa” (alto riesgo no nombrado como IA), exposición concentrada en privacidad (R3 = 406) y vigilancia (R9 = 177), 72,8 % de dependencia de seis firmas estadounidenses. Sobre esa medición derivamos el escudo y señalamos cómo, en general, un acuerdo comercial externo puede prohibir esas leyes antes de que existan.

1. Introducción

Una potencia media que usa IA de frontera no la fabrica: compra semiconductores, cómputo y modelos a un puñado de empresas extranjeras. Por **potencia media** entendemos un Estado que depende de un tercero, otro país o una empresa, para acceder a cómputo, modelos y datos de frontera; no necesariamente carece de todo, pero no controla esas capas. Las doctrinas vigentes no le sirven. La Destrucción Mutua Asegurada (MAD) disuade por castigo, y el Mal Funcionamiento Mutuo Asegurado por IA (MAIM; Hendrycks, Schmidt y Wang 2025), por sabotaje recíproco de centros de datos. Ambas asumen igualdad en poder de cómputo y de regulación, pero México es interdependiente sin ser par y vulnerable sin ser beligerante, de modo que las doctrinas y leyes actuales son insuficientes para garantizarle paridad: ese es el vacío doctrinal.

¹**SARA** = Soberanía Asegurada por Resiliencia Activa; **VIGÍA** = Valoración de Impactos Gubernamentales de Inteligencia Artificial; **MAD** = Destrucción Mutua Asegurada; **MAIM** = Mal Funcionamiento Mutuo Asegurado por IA.

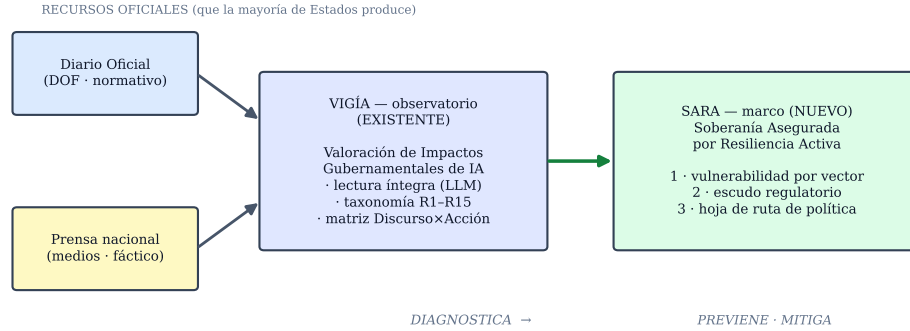


Figura 1: Arquitectura: VIGÍA (autovigilancia, existente) mide y diagnostica; SARA (autorregulación, nuevo) propone, previene y mitiga.

Lo resolvemos con una distinción. Un Estado es soberano sobre un dominio si y solo si puede (a) **fixar reglas vinculantes**, la autorregulación, y (b) **verificar y auditar su cumplimiento**, la autovigilancia. La dependencia retira los **medios de producción** (cómputo, modelos y datos), de modo que esa dimensión queda perdida y la autarquía es inviable. Pero no retira la capacidad legal de fijar reglas ni de auditarlas, porque esa facultad no pertenece a quien es dueño del cómputo. Regular el uso de la dependencia y auditarlo es, entonces, el ejercicio directo de la única dimensión de soberanía que la dependencia no puede quitar: la regulación es la palanca de defensa disponible, y esa es la afirmación central de este trabajo. México entrega a cambio del cómputo dos cosas, sus **datos** nacionales y su **mercado**, y la regulación condiciona y audita ese intercambio para no poner en juego soberanía y seguridad nacional.

De ahí salen dos instrumentos (Fig. 1). **VIGÍA** es el **diagnóstico**, un radar, ya en producción, que mide dónde el Estado no tiene control efectivo sobre la IA que ya usa. **SARA** es la **propuesta de prevención y mitigación**, el escudo de leyes que previene y mitiga el uso de la dependencia como arma. El linaje **MAD** → **MAIM** → **SARA** va de la destrucción y el mal funcionamiento asegurados a la **resiliencia** asegurada. Es una **defensa por capas**, ya que VIGÍA es la primera, ver, y sobre ella se construyen las siguientes, legislar y auditar.

Planteamos tres preguntas. (1) ¿Se puede **medir** la exposición de la soberanía en IA con recursos oficiales del Estado y medios formales? (2) ¿Esa medición se convierte en una **defensa derivable**, no arbitraria, para un Estado sin paridad? (3) ¿El marco es **reproducible** fuera del caso que lo origina? Estas tres preguntas marcan la estructura del documento, en la que cada sección tiene un propósito: la **sección 2** explica el funcionamiento y la medición de VIGÍA; la **sección 3** responde al diagnóstico con propuestas para prevenir y mitigar el riesgo; en la **sección 4** convergen ambos sistemas y se aplican al caso específico de México; y la **sección 5** abre la puerta a profundizar la problemática.

Qué entrega, en concreto. Una dependencia tecnológica puede usarse como palanca de tres maneras: cobrar de más o atar a un proveedor, cortar el servicio, o vigilar y manipular a través de los sistemas que el Estado opera. La dependencia coacciona por sí misma, por precio, por corte o por vigilancia, exista o no una ley; por eso la ausencia de ley es el problema y la ley, la defensa. Frente a cada palanca hay una ley que la neutraliza. El producto del marco es esa correspondencia hecha lista: **un conjunto corto de leyes a aprobar, ordenado por la exposición que VIGÍA mide, con la evidencia de cada punto adjunta**. No es una alerta abstracta, sino una agenda que un legislador puede tomar y ejecutar; la sección 4 la muestra para México.

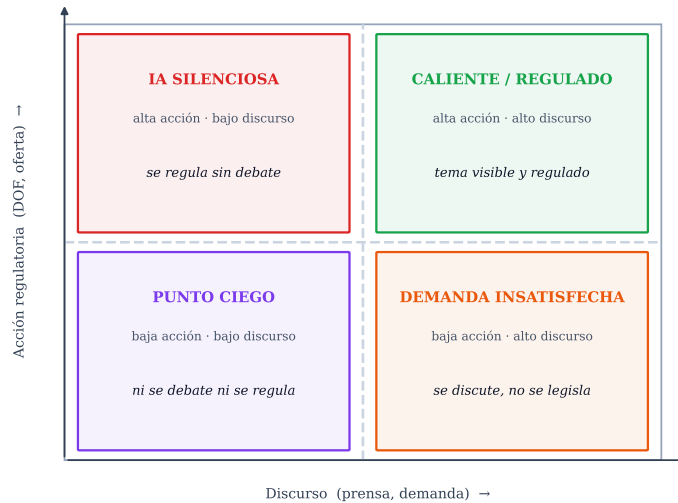


Figura 2: La matriz Discurso×Acción y el significado de cada cuadrante.

2. VIGÍA: la primera capa (el diagnóstico)

Ante esto presentamos el marco, VIGÍA, ya en operación, un observatorio que opera en **dos niveles** y en su **confluencia**. El nivel **normativo** es el diario oficial, la acción regulatoria, lo que el Estado norma. El nivel **fáctico** es la prensa nacional, el discurso público, el registro de cómo se materializa la inseguridad digital en la esfera pública. VIGÍA actúa en la confluencia de ambos, con lectura íntegra de cada nivel más la taxonomía R1–R15, para entregar un diagnóstico de discurso × acción; su aporte es **análisis, diagnóstico y medición**, no solo el *dónde*.

Así VIGÍA captura la **brecha de gobernanza**, el peligro latente que la ciudadanía y los analistas ya perciben en la prensa, pero que el marco legal aún ignora en el diario oficial. Esa brecha existe porque el uso de la tecnología **tácitamente genera riesgo** en distintas materias del derecho, ya que el DOF lo regula a veces sin nombrarlo como IA.

Ambos niveles se leen **íntegros, documento a documento**, con modelos de lenguaje, no por palabras clave, ya que un sistema de alto riesgo casi nunca se nombra “IA”, y un filtro por *keywords* pierde los símiles y los implícitos, la **IA silenciosa**. Esa IA silenciosa es el centro del problema soberano: cuando el Estado opera IA de alto riesgo sin ley que la regule ni auditoría que la verifique, no solo deja un hueco normativo, sino que expone su propia infraestructura crítica y los datos de sus ciudadanos a quien controla esos sistemas. El Estado se vuelve, a la vez, operador y punto vulnerable. Medir esa exposición es el primer acto de soberanía.

Sobre ambos corpus se aplica una taxonomía común de quince categorías, **R1–R15**, de *Fallos y errores* (R1) a *Riesgos emergentes* (R15), incluyendo *Invasión de privacidad* (R3), *Vigilancia autoritaria* (R9) y *Concentración de poder* (R10). La unidad de medida es **funcional**, no nominal, ya que cuenta como IA todo sistema con capacidad de inferencia que impacta a personas o infraestructura, se nombre o no. Sin esto, una ley “de IA” sería letra muerta.

El discurso y la acción se cruzan por categoría y mes en la **matriz Discurso × Acción** (Fig. 2): **IA silenciosa** (alta acción, bajo discurso: se regula sin debate), **Demanda insatisfecha** (alto discurso, baja acción: ventana legislativa del próximo ciclo), **Caliente / regulado** (alto en ambos) y **Punto ciego** (bajo en ambos: riesgo emergente).

La salida de VIGÍA es una **exposición cuantificada por categoría de riesgo**. El método es reproduci-

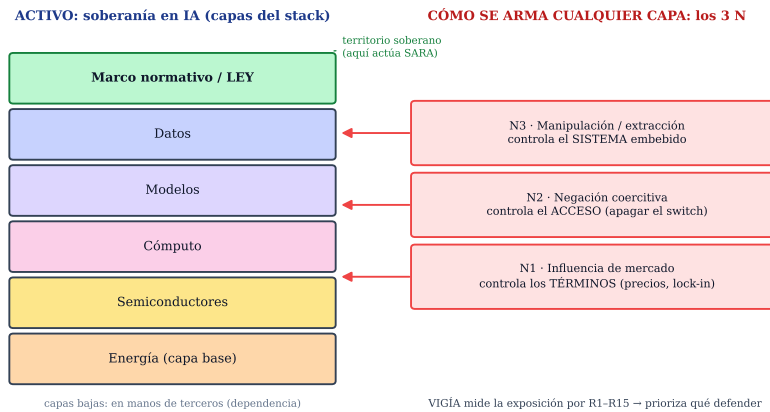


Figura 3: El activo “soberanía” por capas del stack —la ley, en la cima, es territorio soberano— y los tres niveles (3 N) con que se arma cualquier capa.

ble, porque se apoya en recursos oficiales que la mayoría de los Estados democráticos producen. Tenemos el *dónde*. Falta el *cómo* y la *ley*.

3. SARA: de la exposición a las leyes

SARA toma la exposición que mide VIGÍA y, como respuesta al diagnóstico, propone una defensa que previene y mitiga: el activo, cómo puede usarse como arma, y la iniciativa de ley que lo neutraliza.

El activo y las capas. La soberanía en IA es la capacidad de decidir sobre los sistemas en territorio propio sin que un externo pueda **bloquear, alterar o explotar** esa decisión. Se descompone por capas del *stack* (Fig. 3): una potencia media no controla las bajas (energía, semiconductores, cómputo, modelos y datos), pero la superior, el **marco normativo**, es **territorio soberano**, donde SARA actúa.

Los tres niveles (3 N). Toda dependencia confiere al proveedor exactamente tres poderes, según lo único que puede controlar. Son **exhaustivos**, ya que cubren los términos, el acceso, o la cosa misma, y no hay un cuarto, y son crecientes en intrusividad. **N1 · Influencia de mercado:** el proveedor controla los términos {precios, *lock-in* [quedar amarrado a un solo proveedor], cobro excesivo}; el menos intrusivo, el más persistente. En llano, **presión económica** por cobro excesivo o exclusividad. **N2 · Negación coercitiva:** controla el acceso (cortar chips, nube, conexiones de software, actualizaciones); el “apagar el switch”. En llano, **corte de acceso** o servicio. **N3 · Manipulación / extracción activa:** controla el sistema mismo instalado dentro de la infraestructura (monitorear, alterar, sacar datos), como el espionaje tipo Pegasus, el software espía usado contra periodistas y activistas. En llano, **vigilancia y manipulación**. Los 3 N adaptan la *interdependencia armada* de Farrell y Newman (2019), donde su *chokepoint* (negar acceso) corresponde a N2 y su *panopticon* (vigilar desde la red) a N3.

La columna vertebral: **VIGÍA mide la exposición por R1–R15 (el dónde) → los 3 N explican cómo se arma (el cómo) → los 5 pilares cierran cada N (la ley) → de ahí se derivan iniciativas priorizadas**. Una cadena, tres taxonomías y ninguna más.

El escudo: cinco pilares. Cada N es un canal de presión. La propuesta que sigue, como escudo, sigue cinco pilares; cada pilar es una iniciativa de ley que previene y mitiga el uso de un canal, no una intervención normativa directa. Los cinco se **derivan** de cerrar los 3 N, y no son una lista suelta; la dependencia no se elimina, se busca volver **no-armable**, ya que sigue ahí, pero ya no puede usarse como arma de presión (Fig. 4).

Para prevenir y mitigar **N2**, el corte de acceso: **(1) Diversificación**, que exige múltiples proveedores

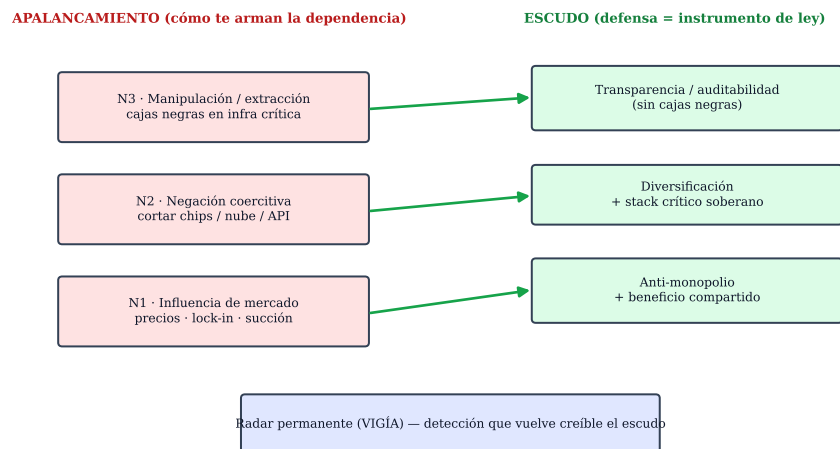


Figura 4: Cada nivel de apalancamiento (N) se cierra con un pilar del escudo, y cada pilar es una ley.

en funciones críticas, de modo que si se corta el acceso a uno el país siga operando, y además ataca el monopolio, al no depender de una sola compañía. Y **(2) Soberanía del stack crítico**, lo que no puede fallar (elecciones, defensa, energía, datos críticos) en capacidad propia o bajo control soberano verificable. Para prevenir y mitigar **N3**, la vigilancia y la manipulación: **(3) Transparencia / auditabilidad**, que prohíbe las cajas negras en sistemas públicos de alto riesgo y da derecho a código y parámetros, porque lo auditado no se manipula en silencio. Para prevenir y mitigar **N1**, la presión económica: **(4) Anti-monopolio**, capacidad regulatoria sobre la concentración en mercados de IA; y **(5) Beneficio compartido**, impuesto digital o de IA y compensación por la minería de datos nacionales.

Los datos no son un sexto pilar. Son la capa **más expuesta**, en México $R3 = 406$, la mayor de todas, y se defienden de forma transversal por los pilares 2 (localización de datos críticos), 3 (auditabilidad) y 5 (compensación). Cinco pilares, no seis.

Protección, no blindaje. El escudo no **bloquea** el acceso, ya que eso es autarquía, imposible, sino que **condiciona y audita** el uso. Da acceso al mercado, pero regula para qué pueden usarse los datos y verifica que se cumpla. La disuasión es regulatoria: el proveedor acepta reglas y auditoría a cambio del acceso. Se materializa en **auditorías algorítmicas obligatorias** y un **órgano auditor descentralizado**, al estilo de la COFEPRIS, la agencia sanitaria mexicana, cuya autonomía lo ata a su mandato, no a la agenda política. Cada pilar es, así, la iniciativa de ley que cierra el vacío medido por VIGÍA.

VIGÍA como radar permanente vuelve creíble el escudo, ya que deja ver el ascenso por la escalera N, de N1 a N3, antes de que sea irreversible, y deja ver el segundo frente. Los pilares son **regulación doméstica**, las leyes que el propio Estado promulga, frente a los acuerdos externos de comercio o estándares, pero un acuerdo externo puede prohibirlas por adelantado: regulación doméstica y negociación externa son el mismo frente, así que conviene legislar antes de negociar.

4. Lo que revela la primera capa (México)

El marco, de punta a punta, en un caso. En el caso aplicado de México, VIGÍA mide que el 72,8% de la IA que nombran las instituciones mexicanas pertenece a seis empresas de EE. UU.; eso es un riesgo de **acceso**, ya que cualquiera podría cortar el servicio. La iniciativa de ley que previene y mitiga ese riesgo es exigir varios proveedores sustituibles en las funciones públicas críticas, para que perder a uno no paralice al Estado. El mismo diagnóstico señala qué pilar proteger, el más expuesto, según la Tabla 2, si un acuerdo externo intentara prohibir esa ley. Lo que sigue generaliza este recorrido a los 665 hallazgos.

Instanciamos el marco. VIGÍA analizó **153 ediciones** del Diario Oficial de la Federación (noviembre 2025 → junio 2026) con lectura íntegra, revisión adversarial y validación determinista (esquema, citas verbatim, conteos): **665 hallazgos** de riesgo de IA, **1 466 etiquetas de riesgo**, **50** marcados de atención urgente. En paralelo clasificó **4 327 notas** de 12 medios en la misma taxonomía R1–R15 y las cruzó en la matriz, abarcando los tres ámbitos que toca la pérdida de soberanía: los recursos que proporciona el sector civil (prensa), el sector privado (demanda empresarial) y el sector público (gobierno, el DOF).

El diagnóstico cuantitativo indica que **el 95,6 %** de los hallazgos del DOF tiene un vacío regulatorio (636/665). **El 82 %** es “IA silenciosa”, alto riesgo regulado sin nombrarse como IA (545/665 implícitos), de modo que una ley activada por mención nominal excluiría el 82 % de los sistemas más riesgosos ya desplegados, lo que **exige una definición funcional**. Operar esos sistemas sin ley ni auditoría es, precisamente, la exposición soberana que la sección 2 describe. Ejemplos: la credencial para votar reconvertida en plataforma biométrica con “interoperabilidad internacional” {Acuerdo INE, abril 2026} y la retención de metadatos de telecomunicaciones por 24 meses {nov 2025, tras el PANAUT [un padrón nacional de usuarios de telefonía móvil con datos biométricos, anulado por la Suprema Corte (SCJN)]}.

La matriz instanciada separa dos cuadrantes accionables (Tabla 1). La prensa **clama** por concentración de poder (R10 = 579), desplazamiento laboral (R7 = 487) y deepfakes (R4 = 360) que el DOF apenas regula (74, 72, 44): **demanda insatisfecha**, ventanas legislativas. El DOF, en cambio, **regula en silencio** privacidad (R3 = 406), sesgo (R2 = 301) y vigilancia (R9 = 177, con 49 hallazgos Muy Alta) con poca prensa: **IA silenciosa**. La exposición se concentra donde la dependencia la predice, y la dependencia es concreta: **el 72,8 %** de las menciones empresariales recae en seis firmas estadounidenses, OpenAI (445), Google (248), Anthropic (230), Nvidia (151), Meta (129) y Microsoft (113).

Tabla: Indicadores del caso México (VIGÍA, nov 2025 – jun 2026).

Indicador	Valor
Ediciones del DOF leídas íntegras	153
Hallazgos de riesgo de IA	665
Etiquetas de riesgo aplicadas	1 466
Notas de prensa clasificadas (12 medios)	4 327
Hallazgos con vacío regulatorio	95,6 % (636/665)
“IA silenciosa” (alto riesgo no nombrado)	82 % (545/665)
Mayor exposición: privacidad (R3)	406 hallazgos
Vigilancia (R9)	177 (49 Muy Alta)
Demanda insatisfecha: concentración (R10, prensa)	579 menciones
R10 en el DOF (feb 2026, tras extinción COFECE/IFT)	1 hallazgo
Punto ciego: desalineación de agentes (R14)	0 DOF / 64 prensa
Dependencia de 6 firmas de EE. UU.	72,8 %

Ante estas dos lecturas se indica un **retroceso que el propio Estado se causó**: R10 cae a **1 hallazgo en febrero 2026**, al extinguirse la COFECE y el IFT, los órganos de competencia y de telecomunicaciones. La concentración no cesó, ya que la prensa la registra con 579 menciones; lo que desapareció fue el órgano que la nombraría: el escalón N1 sin pilar anti-monopolio. Y el **punto ciego extremo**, *Desalineación de agentes* (R14 = 0 en el DOF frente a 64 en prensa); el siguiente riesgo ya asoma en el discurso pero carece de vocabulario regulatorio oficial.

De ese diagnóstico se deriva la propuesta de leyes que sirve como escudo, pilar por pilar: la Tabla 2 alinea cada uno con la iniciativa de ley que cierra el vacío medido y el dato de VIGÍA que lo prioriza, el orden en que conviene legislar.

Tabla: Pilar → ley que lo cierra → dato VIGÍA que lo prioriza.

Pilar (cierra N)	Ley que lo cierra	Dato VIGÍA que lo prioriza
Diversificación (N2)	compras públicas multi-proveedor; sin lock-in crítico	72,8 % de vendors de EE. UU.; Nvidia 151
Stack crítico soberano (N2)	cómputo propio + localización de datos críticos	R3 = 406; credencial INE biométrica
Transparencia / auditabilidad (N3)	derecho a código en alto riesgo; auditoría obligatoria	R9 = 177; precedente Pegasus
Anti-monopolio (N1)	reconstruir capacidad antimonopolio con mandato de IA	R10 = 1 (feb-26); COFECE/IFT extintos
Beneficio compartido (N1)	impuesto digital / IA; compensación por minería	R7 = 487 (prensa, impacto laboral)

5. Discusión

El arco **MAD** → **MAIM** → **SARA** completa una progresión: donde MAD y MAIM disuaden por castigo o sabotaje y exigen paridad, SARA disuade por **denegación**, ya que le niega al proveedor la posibilidad de explotar la dependencia, con la capacidad que la potencia media sí conserva. Es la defensa que previene y mitiga, no una acción agresiva. No es autarquía ni la falsa elección entre depender de EE. UU. o de China, sino **interdependencia regulada**, la tercera vía (Ríos 2026): protegerse de abusos, impedir una IA monopólica y extractiva, y dejar abierta la puerta a tecnología propia. Este artículo entregó la **primera capa**, VIGÍA, ya operativa; el escudo de leyes y su auditoría son las capas que se construyen sobre ella.

De aquí salen tres tareas que se contemplan como respuesta al análisis: **institucionalizar VIGÍA** como radar permanente; **legislar los cinco pilares antes de negociar**, pues un acuerdo externo solo prohíbe lo que aún no existe; y tratar la **soberanía de datos** como transversal, no como pilar suelto. Nada es exclusivo de México: el método ingiere recursos oficiales que la mayoría de los Estados democráticos producen y los 3 N son exhaustivos para cualquier dependencia; el marco es **reproducible** apuntándolo a otro país.

La pérdida de soberanía en datos y vigilancia arrastra pérdida de **autodeterminación democrática**: elecciones permeables a influencia externa e identidad biométrica sin protección. Por eso regular el uso de la IA dependiente no es un trámite técnico, ya que autorregularse y auditar que se cumpla es cómo una potencia media conserva la capacidad de gobernarse a sí misma.

Limitations and Dual-Use Considerations

VIGÍA depende de la lectura por modelos de lenguaje, que puede omitir o malclasificar hallazgos, y su cruce es contemporáneo, por lo que no afirma causalidad; además, los cinco pilares son una derivación argumental, no legislación validada. Sobre el doble uso, el mismo mapa de vacíos y dependencias que orienta la defensa también señala dónde un Estado es vulnerable, así que el reporte se mantiene en un nivel agregado y sin detalle operativo. Como mejoras futuras proponemos la validación externa de los hallazgos, la supervisión humana sistemática y la ampliación a más fuentes y países.

LLM Usage Statement

Usamos modelos de lenguaje (Claude) para la lectura íntegra y la clasificación del diario oficial y la prensa, y como apoyo en la redacción de este reporte; todas las cifras se validaron de forma determinista contra el corpus fuente.

Referencias

Farrell, H. y Newman, A. (2019). *Weaponized Interdependence: How Global Economic Networks Shape State Coercion*. *International Security* 44(1).

Hendrycks, D., Schmidt, E. y Wang, A. (2025). *Superintelligence Strategy*.

Nevo, S. et al. (2024). *Securing AI Model Weights*. RAND, RRA2849-1.

The Feasibility of Training Sovereign Language Models in the Global South: Brazil and Mexico (2025). arXiv:2510.19801.

Algorithmic Sovereignty and the New Security Dependencies (2025).

AI Sovereignty and the Global South's Third Way (2026). *Modern Diplomacy*.

Reglamento (UE) 2024/1689 (EU AI Act).

Ríos, V. (2026). *La trampa de la IA que México no está viendo*. Milenio.