RED IBEROAMERICANA DE PROTECCION DE DATOS

Red Iberoamericana
Rede Ibero-Americana

Elementos mínimos de los procesos de reforma legislativa en materia de protección de datos personales

Para garantizar la protección efectiva de derechos fundamentales

Análisis comparado con énfasis en criterios de agilidad normativa y mecanismos de actualización periódica

*Autor: Luis García Balcarce**

Elaborado en el marco de la Convocatoria "Trabajar en Red" 2025-2026

Septiembre 2026.

Publicado con el apoyo de la Agencia Española de Cooperación Internacional para el Desarrollo AECID

**"Las opiniones, análisis y conclusiones expresados en este documento pertenecen exclusivamente a su autor en calidad de experto independiente y no reflejan necesariamente la postura o criterio de la Red Iberoamericana de Protección de Datos (RIPD). Esta publicación no implica la aprobación de su contenido ni representa la posición institucional de la RIPD, la cual no se hace responsable del uso que pueda darse a la información aquí expuesta."*

Sumario ejecutivo

El acelerado desarrollo de tecnologías de tratamiento masivo de datos, la expansión de la economía digital y la proliferación de sistemas de inteligencia artificial plantean desafíos sin precedente para los marcos normativos de protección de datos personales. En los países iberoamericanos analizados, la mayoría de las legislaciones vigentes presenta una brecha creciente respecto de las referencias contemporáneas, lo que genera incertidumbre jurídica, déficits en la protección efectiva de derechos fundamentales y obstáculos para la cooperación transfronteriza.

El presente documento de referencia sistematiza los elementos mínimos que deben integrar todo proceso de reforma legislativa en materia de protección de datos personales para garantizar la protección efectiva de derechos fundamentales. Se basa en el análisis comparado de los marcos normativos vigentes y los proyectos de reforma de seis países: Argentina, Brasil, Chile, Ecuador, México y Uruguay. Estas jurisdicciones constituyen una muestra no exhaustiva del espacio iberoamericano. Ello no obsta a las referencias puntuales a otros ordenamientos de la región que se incluyen a lo largo del documento. Además, se ofrecen criterios de agilidad normativa y mecanismos de actualización periódica orientados a que las legislaciones puedan acompañar el ritmo de las tecnologías emergentes.

Las conclusiones principales del análisis indican que: (i) ninguno de los marcos analizados cumple en su totalidad con los estándares contemporáneos, aunque existen avances significativos en los casos de Brasil, Chile y Uruguay; (ii) en esos marcos, la regulación de la inteligencia artificial y las decisiones automatizadas constituye la brecha más extendida; (iii) en los países analizados, la independencia institucional de la autoridad de control es el factor con mayor incidencia en la eficacia real del sistema de protección; y (iv) los mecanismos de actualización periódica -revisiones obligatorias y habilitaciones normativas delegadas con base legal expresa- son indispensables para preservar la vigencia de las legislaciones en el tiempo, y pueden complementarse con propuestas de lege ferenda como las cláusulas de caducidad tecnológica.

1. Introducción y alcance del documento

La protección de datos personales ha evolucionado de ser una garantía instrumental asociada a la privacidad individual hacia convertirse en una condición estructural del Estado democrático de derecho en la era digital. Su efectividad depende no solo de la existencia de una norma legal, sino de la calidad jurídica de esa norma: su cobertura material, el equilibrio entre sus mandatos y excepciones, la solidez institucional de su autoridad de aplicación y, cada vez más, su capacidad de adaptarse al cambio tecnológico ante procesos legislativos largos y complejos.

El presente documento responde a un doble objetivo. En primer lugar, ofrece un análisis comparado actualizado de los marcos normativos en materia de protección de datos personales en seis países iberoamericanos: Argentina, Brasil, Chile, Ecuador, México y Uruguay. Se presta especial atención a los proyectos de reforma legislativa en curso y a las reformas institucionales recientes, algunos de los cuales representan avances significativos, mientras que otros presentan desafíos y aspectos que requieren especial consideración. En segundo término, sistematiza un conjunto de elementos mínimos -organizados en diez categorías temáticas- que todo proceso de reforma legislativa en la materia debe contemplar para garantizar la protección efectiva de derechos fundamentales.

El análisis comparado se circunscribe a seis jurisdicciones: Argentina, Brasil, Chile, Ecuador, México y Uruguay. Estas jurisdicciones constituyen una muestra del espacio iberoamericano.

El documento distingue dos tipos de contenidos. Los estándares jurídicos consolidados son aquellos que ya cuentan con reconocimiento en instrumentos de referencia, como el Reglamento General de Protección de Datos de la Unión Europea, el Convenio 108+ o los Estándares Iberoamericanos de la RIPD. Las propuestas de *lege ferenda* son medidas de política legislativa que el documento recomienda, pero que no constituyen hoy un estándar consolidado. Estas últimas se identifican en el texto con la indicación "*(propuesta de lege ferenda)*".

El documento incorpora, además, un análisis específico de los criterios de agilidad normativa y los mecanismos de actualización periódica que permiten a las legislaciones acompañar el ritmo de las tecnologías emergentes sin perder coherencia ni certeza jurídica. Este aspecto es particularmente relevante en el contexto actual, caracterizado por la expansión de la inteligencia artificial generativa, el tratamiento masivo de datos biométricos y neuronales, y el desarrollo de los espacios de datos transfronterizos.

El documento ha sido elaborado en el marco de la **Convocatoria "Trabajar en Red" 2025-2026** de la SEGIB y del **Observatorios Iberoamericano de Protección de Datos de la RIPD**, que incorpora como prioridades la intersección entre inteligencia artificial y protección de datos, los tratamientos biométricos y la protección de colectivos vulnerables.

2. Marco conceptual: derechos fundamentales y protección de datos

La protección de datos personales ha adquirido en el derecho iberoamericano un reconocimiento progresivo como derecho fundamental autónomo, diferenciado -aunque estrechamente vinculado- del derecho a la privacidad. Esta configuración encuentra su formulación paradigmática en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea, y ha sido posteriormente recogida y desarrollada en instrumentos de soft law regionales, como los recientemente aprobados Estándares de la Red Iberoamericana de Protección de Datos[1], así como en marcos internacionales más amplios, como la Recomendación de la UNESCO sobre la Ética de la Inteligencia Artificial (2021), que refuerzan su centralidad en la gobernanza contemporánea de los datos.

Desde esta perspectiva, la protección de datos personales no es únicamente una garantía individual frente al tratamiento abusivo de información, sino también un presupuesto del ejercicio de otros derechos fundamentales: la libertad de expresión, la no discriminación, el acceso a la justicia, la igualdad ante la ley y la participación política.

La Carta Iberoamericana de Principios y Derechos en los Entornos Digitales (CIPDED), adoptada en el marco de la Secretaría General Iberoamericana (SEGIB), y los Estándares Iberoamericanos de Protección de Datos Personales de la Red Iberoamericana de Protección de Datos (RIPD) constituyen instrumentos de referencia de alcance regional que enmarcan los análisis contenidos en este documento. Ambos forman parte de un ecosistema que orienta la convergencia normativa en materia de derechos digitales en Iberoamérica.

Los principios fundamentales que estructuran los marcos normativos contemporáneos de protección de datos, reconocidos tanto en el Reglamento General de Protección de Datos de la Unión Europea como en los Estándares Iberoamericanos de la RIPD, comprenden la licitud, lealtad y transparencia; la limitación de la finalidad; la minimización de datos; la exactitud; la limitación del plazo de conservación; la integridad y confidencialidad; y la responsabilidad proactiva. Estos principios operan como reglas generales de carácter transversal, que informan e integran todo el sistema y resultan aplicables a cualquier tratamiento de datos personales, salvo en los supuestos excepcionales expresamente previstos.

[1] https://www.redipd.org/documento/estandares-iberoamericanos-2026.pdf

3. Panorama iberoamericano: diagnóstico comparado de seis jurisdicciones

El siguiente cuadro ofrece una visión de conjunto del estado normativo e institucional en materia de protección de datos personales en los seis países objeto de este análisis. La tabla identifica el marco legal vigente, el estado de los procesos de reforma y los aspectos más destacados de cada sistema.

País	Marco vigente	Estado de reforma	Aspectos destacados
Argentina	Ley 25.326 (2000)	Proyecto de reforma (Mensaje 87/2023) sin sanción. Nuevas mesas de diálogo público-privado para reenviar el proyecto al Congreso Nacional.	Proceso participativo amplio mediante consulta pública y 11 mesas de diálogo (173 aportes). Proyecto de ley en proceso de actualización por la AAIP para su presentación. Propuesta de modificación también incluida en Exp. 2130-D-2025 sobre IA. Adecuación UE reconocida.
Brasil	LGPD – Ley 13.709 (2018, vigente desde 2020)	ANPD regula mediante resoluciones. Transformada en agencia reguladora por la Ley N° 15.352/2026	ANPD con autonomía reforzada desde 2022 y transformada en agencia reguladora por la Ley N° 15.352/2026. Regulación de IA en debate. Adecuación UE reconocida. Estatuto Digital del Niño y del Adolescente (ECA Digital), Ley N° 15.211/2025. Modificación del Marco Civil de Internet por Decreto N° 12.975/2026. Medidas de protección de las mujeres en entornos digitales, Decreto N° 12.976/2026.
Chile	Ley 21.719 (promulgada dic. 2024; vigencia dic. 2026)	Ley nueva ya aprobada; en período de adecuación. Proyecto de modificación en tramitación (boletín 18623-07, septiembre de 2026)	Al menos siete años de tramitación legislativa, desde los boletines refundidos de 2017. Crea Agencia autónoma. Alineada al RGPD.
Ecuador	Ley Orgánica de Protección de Datos Personales – LOPDP (2021)	En implementación, con Reglamento General de la LOPDP vigente desde noviembre de 2023 y normativa secundaria de la SPDP expedida durante 2024, 2025 y 2026	Exige delegado de protección de datos personales (DPD) en las entidades públicas y, en el sector privado, en los supuestos previstos por la LOPDP y la normativa secundaria. Autoridad de control creada. Transferencias internacionales reguladas, con reconocimiento de las cláusulas contractuales modelo de la RIPD.

País	Marco vigente	Estado de reforma	Aspectos destacados
			Norma vinculante sobre datos personales en sistemas de IA, con gestión de riesgos, evaluación de impacto y auditorías.
México	LGPDPPSO y LFPDPPP (2025)	Reforma constitucional de diciembre de 2024: extinción del INAI. Leyes nuevas en vigor desde el 21/03/2025. Proceso de actualización de la LFPDPPP en curso	Extinción del organismo constitucional autónomo. Atribuciones transferidas a la Secretaría Anticorrupción y Buen Gobierno, que las ejerce a través de la Unidad de Protección de Datos Personales.
Uruguay	Ley 18.331 (2008), reformada por Ley 19.670 (2018)	Sin reforma integral reciente; actualizaciones por resoluciones de la URCDP	Marco maduro con DPO obligatorio, DPIA, privacidad por diseño. URCDP activa en cooperación regional. Adecuación UE reconocida.

3.1. Argentina

La Ley 25.326 de Protección de Datos Personales, sancionada en el año 2000, fue pionera en el contexto regional al establecer un marco integral y al habilitar la primera declaración de adecuación al nivel europeo de protección en el año 2003. La norma establece los principios, derechos y obligaciones aplicables al tratamiento de datos personales en Argentina.

No obstante, frente a las transformaciones del ecosistema digital y al avance de la economía basada en datos, el régimen vigente presenta ciertos desafíos y limitaciones regulatorias. En particular, la ley no incorpora disposiciones específicas sobre decisiones automatizadas, no contempla el principio de responsabilidad proactiva ni la figura del delegado de protección de datos (DPO). Asimismo, el régimen de transferencias internacionales previsto en la Ley N° 25.326 responde a un contexto previo a la actual intensificación y complejidad de los flujos transfronterizos de datos.

La Agencia de Acceso a la Información Pública (AAIP), autoridad de aplicación y control de la Ley 25.326 impulsó en 2022 un proceso participativo amplio, con once mesas de diálogo nacionales e internacionales y una consulta pública que recibió 173 documentos con aportes y comentarios de 123 participantes, para la posterior elaboración de un anteproyecto de ley. El Poder Ejecutivo remitió el Mensaje 87/2023 con el proyecto de ley a la Cámara de Diputados, pero la iniciativa no ha sido tratada en el Congreso. A partir de esa iniciativa, entre el 2025 y el año en curso la AAIP se encuentra trabajando en un proyecto de actualización del proyecto del 2023, a través de nuevas mesas de diálogo público-privado.

Paralelamente, el proyecto de ley marco sobre inteligencia artificial (Expediente 2130-D-2025) propone ampliar definiciones clave de la Ley 25.326 para incluir datos sensibles e inferencia algorítmica. La actualización de la ley de protección de datos es considerada por diversos actores legislativos como un

paso previo indispensable para cualquier regulación específica de inteligencia artificial, dado que los sistemas de IA dependen fundamentalmente del tratamiento de datos personales.

Asimismo, la Argentina ratificó el Convenio 108+, único instrumento jurídicamente vinculante en materia de protección de datos personales y aprobó en octubre de 2023 las cláusulas contractuales modelo de la RIPD para transferencias internacionales (Resolución 198/2023), convirtiéndose en el tercer país de la región, junto con Uruguay y Perú, en adoptar este instrumento. Recientemente Colombia también las aprobó. En el caso de Ecuador, la SPDP reconoció las cláusulas contractuales modelo de la RIPD mediante la Resolución Nº SPDP-SPD-2026-0004-R, con las particularidades y excepciones previstas en esa resolución. Argentina revalidó en 2024 la decisión de adecuación con la Unión Europea bajo el GDPR lo que facilita considerablemente los flujos transfronterizos de datos con el espacio europeo.

3.2. Brasil

Brasil cuenta con la Ley General de Protección de Datos (LGPD - Lei 13.709/2018), en vigor desde 2020. La LGPD contempla principios alineados al RGPD, bases legítimas de tratamiento diferenciadas del consentimiento, régimen específico para datos sensibles, derechos ampliados de los titulares y un régimen sancionatorio progresivo. Además, a partir de principios del 2026, Brasil cuenta con la Adecuación reconocida por la Unión Europea.

El marco se completó con normas sectoriales posteriores: el Estatuto Digital del Niño y del Adolescente (ECA Digital), aprobado por la Ley N° 15.211/2025, la modificación del Marco Civil de Internet por el Decreto N° 12.975/2026 y las medidas de protección de las mujeres en entornos digitales del Decreto N° 12.976/2026.

La Autoridade Nacional de Proteção de Dados (ANPD) fue creada por la LGPD y ha ido consolidando su autonomía funcional y normativa mediante la emisión de regulaciones sectoriales. La Ley N° 15.352/2026 la transformó en agencia reguladora.

3.3. Chile

Chile completó en diciembre de 2024 un proceso de reforma legislativa de al menos siete años de duración, con la promulgación de la Ley 21.719 de Protección y Tratamiento de Datos Personales. La tramitación se inició con dos proyectos presentados en 2017, posteriormente refundidos: el boletín 11092-07, de 17 de enero de 2017, y el boletín 11144-07, de 15 de marzo de 2017. Esta norma reemplaza la Ley 19.628 de 1999 y entrará en vigencia en diciembre de 2026. El 1 de septiembre de 2026 se presentó un proyecto de ley que busca modificarla (boletín 18623-07), actualmente en tramitación.

La Ley 21.719 incorpora la creación de la Agencia de Protección de Datos Personales como organismo autónomo con facultades para dictar instrucciones, fiscalizar y sancionar; regulación de las decisiones automatizadas con efectos jurídicos significativos; régimen de evaluación de impacto en la privacidad; designación de un delegado de protección de datos personales, obligatoria únicamente como parte de la adopción del modelo de prevención de infracciones regulado en el artículo 49 de la ley; y un sistema

de transferencias internacionales basado en la adecuación o en garantías adecuadas. La fuente principal de inspiración es el RGPD europeo, adaptado a las particularidades del ordenamiento jurídico chileno.

3.4. Ecuador

Ecuador aprobó en 2021 la Ley Orgánica de Protección de Datos Personales (LOPDP), publicada en el Quinto Suplemento del Registro Oficial Nº 459, de 26 de mayo de 2021, que dotó al país de un marco normativo alineado en buena medida con los estándares del RGPD europeo y los Estándares Iberoamericanos de la RIPD. La LOPDP establece principios de tratamiento, derechos de los titulares, bases legítimas diferenciadas, un régimen específico para datos sensibles y la designación del delegado de protección de datos personales (DPD) en las entidades públicas y, en el sector privado, en los supuestos previstos por la propia ley y por la normativa secundaria, en particular el Reglamento del Delegado de Protección de Datos Personales (Resolución Nº SPDP-SPD-2025-0028-R). El marco se completa con el Reglamento General de la LOPDP, vigente desde noviembre de 2023, y con la normativa secundaria expedida por la Superintendencia de Protección de Datos Personales (SPDP) durante 2024, 2025 y 2026. Además, en febrero de 2026 el Superintendente de Protección de Datos Personales expidió la Resolución Nº SPDP-SPD-2026-0009-R, mediante la cual aprobó la Norma General para la Garantía del Derecho de Protección de Datos Personales en el Uso de Sistemas de Inteligencia Artificial, reformada por la Resolución Nº SPDP-SPD-2026-0037-R, que precisa el alcance de las obligaciones aplicables a responsables y encargados del tratamiento en el uso de sistemas de inteligencia artificial. Esa norma no se limita a declarar aplicable la LOPDP a la inteligencia artificial: establece expresamente la gestión de riesgos, la evaluación de impacto cuando proceda y la realización de auditorías respecto de los sistemas de IA que tratan datos personales, conforme a la LOPDP, su Reglamento General y la normativa secundaria.

3.5. México

La reforma constitucional publicada en diciembre de 2024, en el marco del proceso denominado 'Simplificación Orgánica', dispuso la extinción del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), organismo constitucional autónomo cuyas atribuciones fueron transferidas, en el ámbito correspondiente, a la Secretaría Anticorrupción y Buen Gobierno. El marco normativo vigente en materia de protección de datos personales se integra primordialmente por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y la Ley Federal de Protección de Datos Personales en Posesión de Particulares, ordenamientos que entraron en vigor en marzo de 2025.

México es Parte del Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal (Convenio 108) y de su Protocolo Adicional. Se encuentra en curso un proceso de actualización de la Ley Federal de Protección de Datos Personales en Posesión de Particulares, que contempla la incorporación de categorías especiales de datos personales, el derecho a no ser objeto de decisiones basadas exclusivamente en tratamientos automatizados, el derecho a la limitación del tratamiento, la designación de un oficial de protección de datos personales, la regulación de las transferencias internacionales mediante garantías adecuadas y criterios de nivel de

protección adecuado, el desarrollo de bases jurídicas para el tratamiento, las evaluaciones de impacto, la notificación de vulneraciones de seguridad a la autoridad competente, la privacidad desde el diseño y por defecto, y la implementación de espacios de experimentación regulatoria. La propuesta incorpora además disposiciones sobre tecnologías emergentes, incluida la inteligencia artificial, en los supuestos que involucren tratamiento de datos personales.

3.6. Uruguay

Uruguay cuenta con la Ley 18.331 de 2008, reformada significativamente por la Ley 19.670 de 2018 -que incorporó disposiciones inspiradas en el RGPD, incluyendo la figura del DPO, la evaluación de impacto en la privacidad y el principio de responsabilidad proactiva-, establece un sistema administrado por la Unidad Reguladora y de Control de Datos Personales (URCDP).

Uruguay cuenta con una declaración de adecuación de la Unión Europea, lo que facilita considerablemente los flujos transfronterizos de datos con el espacio europeo. La URCDP ha emitido resoluciones sobre transferencias internacionales, notificación de brechas de seguridad, DPO y marcos de privacidad.

Además, Uruguay ha adoptado las cláusulas contractuales modelo para transferencias internacionales de datos.

4. Elementos mínimos de toda reforma legislativa en protección de datos

El análisis comparado de los marcos normativos comparados permite identificar diez categorías temáticas que deben integrar todo proceso de reforma legislativa en materia de protección de datos personales para garantizar la protección efectiva de derechos fundamentales. Estas categorías son complementarias entre sí y no tienen un orden jerárquico rígido, aunque los elementos relativos a la autoridad de control y los fundamentos constitucionales revisten carácter estructural respecto del resto del sistema.

4.1. Fundamentos constitucionales y de derechos humanos

Todo marco normativo de protección de datos debe anclar su fundamento en el reconocimiento expreso de la protección de datos personales como derecho fundamental e inescindible del catálogo de derechos inherentes a la persona humana en el entorno digital. Este anclaje constitucional es condición de posibilidad para la interpretación favorable al titular de datos en caso de conflicto normativo y para la tutela judicial efectiva del derecho.

Elementos mínimos en esta categoría:

- Reconocimiento expreso del derecho a la protección de datos personales, ya sea en el texto constitucional o mediante remisión normativa a instrumentos internacionales de rango constitucional.

- Incorporación del enfoque de derechos humanos como criterio de interpretación de toda la legislación derivada.

- Articulación con los mecanismos de protección de derechos fundamentales existentes en el ordenamiento jurídico (habeas data, amparo, acción de protección u equivalentes).

- Reconocimiento de la dimensión colectiva del derecho, sin limitarse a la protección de datos de personas físicas individuales.

4.2. Principios rectores del tratamiento

Los principios rectores constituyen el núcleo normativo irrenunciable de toda legislación de protección de datos. Operan como cláusulas generales de aplicación supletoria para situaciones no expresamente previstas y como parámetro de interpretación de las reglas específicas. Su consagración debe ser suficientemente precisa para generar obligaciones jurídicas exigibles, y suficientemente general para cubrir tecnologías y modalidades de tratamiento aún no conocidas.

Los principios mínimos que se listan a continuación se basan en el Art. 5 del RGPD y en los Estándares Iberoamericanos RIPD (2026):

- Licitud, lealtad y transparencia: el tratamiento debe tener una base jurídica habilitante, realizarse de manera leal con el titular y de modo inteligible para éste.

- Limitación de la finalidad: los datos sólo pueden tratarse para los fines determinados, explícitos y legítimos para los que fueron recopilados.

- Minimización de datos: sólo deben tratarse los datos adecuados, pertinentes y limitados a lo necesario para los fines declarados.

- Exactitud: los datos deben ser exactos y, en su caso, actualizados; los datos inexactos deben suprimirse o rectificarse sin dilación.

- Limitación del plazo de conservación: los datos no deben mantenerse más tiempo del necesario para los fines del tratamiento.

- Integridad y confidencialidad: deben adoptarse medidas técnicas y organizativas adecuadas para garantizar la seguridad de los datos.

- Responsabilidad proactiva (accountability): el responsable del tratamiento debe estar en condiciones de demostrar el cumplimiento de todos los principios anteriores.

4.3. Derechos de los titulares de datos

El efectivo ejercicio de los derechos por parte de los titulares de datos es el indicador más directo de la eficacia real de una legislación de protección de datos. La regulación de estos derechos debe incluir procedimientos claros de ejercicio, plazos de respuesta definidos, gratuidad como regla general, y mecanismos de reclamación ante la autoridad de control cuando el responsable no atienda las solicitudes en debida forma.

Derechos mínimos exigibles:

- Derecho de acceso: conocer qué datos se tratan, con qué finalidad, durante qué período y quiénes son los destinatarios.

- Derecho de rectificación: corregir datos inexactos o incompletos.

- Derecho de supresión: eliminar datos cuando ya no sean necesarios, se retire el consentimiento, o el tratamiento resulte ilícito.

- Derecho de limitación del tratamiento: suspender temporalmente el tratamiento en determinadas circunstancias.

- Derecho de portabilidad: recibir los datos en formato estructurado, de uso común y lectura mecánica, y transmitirlos a otro responsable.

- Derecho de oposición: oponerse al tratamiento por motivos relacionados con la situación particular del titular.

- Derecho a no ser objeto de decisiones automatizadas con efectos significativos, sin intervención humana significativa (véase 4.8).

- Derecho a la información: ser informado de manera previa, concisa, transparente e inteligible sobre todas las condiciones del tratamiento.

4.4. Bases legítimas de tratamiento y consentimiento

La diversificación de las bases legítimas de tratamiento es uno de los elementos que distingue los marcos normativos de nueva generación de los marcos más antiguos, que privilegiaban el consentimiento como base casi exclusiva. Un sistema basado únicamente en el consentimiento resulta inadecuado para regular el tratamiento de datos en contextos de desequilibrio de poder entre el titular y el responsable, y genera ficciones de voluntariedad que no se corresponden con la realidad de las interacciones digitales.

Bases legítimas mínimas que debe contemplar toda reforma:

- Consentimiento libre, específico, informado, inequívoco y, en el caso de datos sensibles, expreso.
- Ejecución de un contrato del que el titular es parte.
- Cumplimiento de una obligación legal o reglamentaria del responsable.
- Protección de intereses vitales del titular o de otra persona física.
- Cumplimiento de una misión en interés público o ejercicio de poderes públicos conferidos al responsable.
- Intereses legítimos perseguidos por el responsable, siempre que no prevalezcan sobre los derechos del titular.

El consentimiento, cuando sea la base habilitante, debe poder retirarse en cualquier momento y la forma de hacerlo debe ser igual de sencilla que su otorgamiento. Las legislaciones deben regular específicamente el tratamiento de datos de personas menores de edad, estableciendo umbrales de edad para el consentimiento autónomo y las condiciones del consentimiento parental. Brasil adoptó un régimen específico en la materia mediante el Estatuto Digital del Niño y del Adolescente (Ley N° 15.211/2025).

4.5. Datos sensibles, categorías especiales y regímenes específicos

Las categorías especiales de datos, aquellos cuyo tratamiento entraña riesgos especialmente elevados para los derechos y libertades fundamentales, requieren un régimen de protección reforzado, que incluya una enumeración de categorías, la prohibición por regla general de su tratamiento y la previsión de excepciones específicas y sujetas a garantías adicionales.

Categorías especiales mínimas:

- Origen racial o étnico.
- Opiniones políticas, convicciones religiosas, filosóficas o morales.
- Afiliación sindical.
- Datos genéticos y biométricos cuando se utilicen para identificar de manera unívoca a una persona física.
- Datos relativos a la salud, incluida la salud mental.
- Datos relativos a la vida sexual u orientación sexual.

Otras categorías de datos no integran las categorías especiales, pero están sometidas a un régimen específico o reforzado. Es el caso de los datos relativos a condenas e infracciones penales. Su tratamiento requiere reglas propias, diferenciadas de las aplicables a las categorías especiales, que delimiten los sujetos habilitados para tratarlos y las garantías exigibles.

Las legislaciones de nueva generación incorporan además categorías emergentes de especial sensibilidad, como los datos neuronales y de actividad cerebral (neuroderechos). Otras realidades emergentes reciben un tratamiento reforzado sin integrarse necesariamente en las categorías especiales: los datos de geolocalización de precisión, los perfiles inferenciales generados por sistemas de IA y los datos de menores en entornos educativos y recreativos digitales. Toda reforma legislativa debe prever un mecanismo para incorporar nuevas categorías sin necesidad de una reforma completa de la ley. Cuando ese mecanismo consista en una habilitación a la autoridad de control, debe fundarse en una habilitación legal expresa y respetar los límites constitucionales de cada ordenamiento (véase 5.2).

4.6. Transferencias internacionales de datos

El régimen de transferencias internacionales de datos determina en qué condiciones pueden circular datos personales hacia territorios o entidades receptoras que están fuera del ámbito de aplicación de la ley. La regulación de esta cuestión es particularmente relevante en el contexto iberoamericano, dado el elevado volumen de datos que fluyen entre países de la región y hacia jurisdicciones extrarregionales, en particular a través de plataformas digitales globales.

Elementos mínimos del régimen de transferencias internacionales:

- Prohibición general de transferencias a jurisdicciones que no ofrezcan un nivel de protección equivalente al nacional, salvo excepciones específicas.
- Mecanismo de determinación de la adecuación de terceros países, a cargo del órgano que cada ordenamiento designe como competente, con criterios transparentes y revisión periódica.
- Instrumentos alternativos de garantía: cláusulas contractuales tipo (modelo RIPD), reglas corporativas vinculantes, certificaciones reconocidas.
- Excepciones taxativas para supuestos justificados: consentimiento explícito del titular, ejecución de contratos, interés público, ejercicio de derechos en procedimientos judiciales.
- Cooperación entre autoridades de control para la supervisión de flujos transfronterizos.

4.7. Responsabilidad proactiva y diseño basado en privacidad

El principio de responsabilidad proactiva (accountability) implica un cambio de paradigma respecto de los marcos normativos anteriores: el responsable del tratamiento ya no puede limitarse a cumplir formalmente con la ley, sino que debe poder demostrar en todo momento el cumplimiento efectivo de sus obligaciones. Este principio opera como fundamento de todo el sistema de obligaciones preventivas y organizativas que la legislación impone al responsable.

Obligaciones mínimas derivadas de la responsabilidad proactiva:

- Registro de actividades de tratamiento: documentación sistemática de todas las operaciones de tratamiento realizadas.
- Privacidad desde el diseño (Privacy by Design): incorporación de medidas técnicas y organizativas de protección de datos desde la fase de diseño de sistemas y productos.

- Privacidad por defecto (Privacy by Default): configuración de los sistemas de manera que, por defecto, solo se traten los datos estrictamente necesarios para cada finalidad.

- Evaluación de Impacto en la Protección de Datos (EIPD / DPIA): obligatoria cuando el tratamiento pueda entrañar un alto riesgo para los derechos y libertades de los titulares.

- Designación de Delegado de Protección de Datos (DPO): obligatoria para entidades públicas y para organizaciones privadas que realicen tratamientos a gran escala o de datos sensibles como actividad principal.

- Notificación de brechas de seguridad: a la autoridad de control en un plazo máximo (72 horas en el estándar RGPD) y al titular cuando la brecha pueda suponer un alto riesgo.

- Política de protección de datos documentada y comunicada a todos los niveles de la organización.

4.8. Decisiones automatizadas e inteligencia artificial

La regulación de las decisiones adoptadas total o parcialmente por sistemas automatizados, incluidos los sistemas de inteligencia artificial, constituye la laguna normativa más extendida en los marcos analizados y uno de los desafíos regulatorios más urgentes. La capacidad de los sistemas de IA para inferir atributos sensibles, generar perfiles de comportamiento y adoptar decisiones con efectos jurídicos significativos sobre las personas hace imprescindible un marco normativo específico.

Elementos mínimos para la regulación de decisiones automatizadas:

- Derecho a no ser objeto de decisiones basadas exclusivamente en tratamiento automatizado, incluida la elaboración de perfiles, que produzcan efectos jurídicos o afecten significativamente a la persona.

- Excepciones taxativas al derecho anterior: ejecución de contratos, autorización legal expresa con garantías adecuadas, consentimiento explícito del titular.

- Garantías mínimas en los casos exceptuados: derecho a obtener intervención humana significativa, expresar el punto de vista e impugnar la decisión.

- Obligaciones de transparencia sobre la lógica del algoritmo, sus efectos previstos y el impacto de la decisión para el titular.

- Prohibición de decisiones automatizadas basadas en categorías especiales de datos, salvo consentimiento explícito o razones de interés público con garantías adecuadas.

- Evaluación de impacto algorítmico como obligación previa al despliegue de sistemas de IA con capacidad de adoptar decisiones que afecten significativamente a las personas.

- Mecanismo de articulación con la regulación sectorial de IA, cuando ésta exista, para garantizar coherencia normativa.

- Derecho a la explicación de las decisiones automatizadas.

- Auditorías externas para sistemas de alto riesgo. Algunos ordenamientos ya exigen auditorías de los sistemas de IA sin requerir que sean externas (propuesta de lege ferenda en cuanto al carácter externo).

El proyecto de regulación de IA de Argentina (Exp. 2130-D-2025) incorpora la inferencia algorítmica como categoría de dato sensible, lo que supone un avance significativo respecto de la Ley de Protección de Datos Personales de ese país. Ecuador cuenta con regulación vigente en la materia: la Resolución Nº SPDP-SPD-2026-0009-R, reformada por la Resolución Nº SPDP-SPD-2026-0037-R, exige gestión de riesgos, evaluación de impacto cuando proceda y auditorías respecto de los sistemas de IA que tratan datos personales. Chile, Brasil y Uruguay contemplan en sus marcos vigentes o en proceso de reforma disposiciones específicas sobre este ámbito.

4.9. Autoridad de control

La experiencia comparada de los países analizados demuestra que la existencia de una autoridad de control efectiva, independiente y con recursos adecuados es la variable con mayor incidencia en la eficacia real del sistema de protección de datos.

Características mínimas de la autoridad de control:

- Independencia funcional, orgánica y presupuestaria respecto del Poder Ejecutivo y de los sujetos regulados.

- Estatuto jurídico que garantice la estabilidad de sus miembros y su inamovilidad durante el mandato, salvo causales taxativas y sujetas a control judicial.

- Atribuciones suficientes: supervisión, investigación, dictado de normas, resolución de reclamos y aplicación de sanciones.

- Facultad de interponer acciones frente a normas que vulneren el derecho a la protección de datos.
- Recursos humanos, técnicos y presupuestarios proporcionales a la dimensión del mercado y la complejidad de las tecnologías que debe regular.
- Cooperación con otras autoridades de control nacionales e internacionales, como por ejemplo en el marco de la RIPD.
- Publicidad de sus decisiones y criterios, con vocación de servir como guía de cumplimiento para los responsables del tratamiento.
- Régimen de rendición de cuentas ante el Parlamento, sin subordinación jerárquica a éste (propuesta de lege ferenda).

4.10. Régimen sancionatorio y recursos jurisdiccionales

Un régimen sancionatorio creíble y proporcionado es condición necesaria para la efectividad disuasoria del marco normativo. La experiencia del RGPD europeo y de las autoridades de los países analizados, demuestra que la combinación de sanciones administrativas elevadas, publicidad de las resoluciones y capacidad de acción de oficio es más disuasoria que el monto nominal de la sanción máxima.

Elementos mínimos del régimen sancionatorio:

- Tipificación de infracciones leves, graves y muy graves, con criterios de graduación claros (naturaleza, gravedad, duración, carácter intencional o negligente, número de afectados).
- Sanciones administrativas proporcionales, disuasorias y efectivas. El estándar internacional de referencia vincula las sanciones máximas al volumen de negocios del responsable.
- Publicidad de las resoluciones sancionatorias, con anonimización de los datos de los titulares afectados cuando corresponda.
- Acción de oficio por parte de la autoridad de control, sin necesidad de reclamo previo del titular.
- Derecho a la tutela judicial efectiva del titular de datos, incluyendo la posibilidad de impugnar judicialmente las decisiones de la autoridad de control.

- Acción colectiva o representación por organizaciones de defensa de consumidores y derechos digitales, en condiciones análogas a las acciones individuales.

- Responsabilidad civil del responsable del tratamiento por los daños y perjuicios causados al titular de datos, con inversión de la carga de la prueba.

5. Criterios de agilidad normativa

La velocidad de evolución tecnológica en el campo del tratamiento de datos plantea un desafío estructural a la técnica legislativa tradicional: los marcos normativos sancionados a través de procedimientos parlamentarios completos tienden a quedar desactualizados con rapidez, y las reformas legislativas exhaustivas implican plazos incompatibles con el ritmo de los cambios tecnológicos. La respuesta a este desafío requiere un conjunto de criterios de diseño normativo que integren agilidad y certeza jurídica.

5.1 Arquitectura normativa en capas

El diseño óptimo de una legislación de protección de datos en el contexto actual adopta una arquitectura en capas o niveles, que distingue entre:

- Ley marco o estatutaria: establece principios, derechos, estructura institucional y régimen sancionatorio. Solo se modifica por procedimiento legislativo ordinario, lo que le confiere estabilidad y certeza jurídica.

- Reglamentación de desarrollo: desarrolla aspectos técnicos y procedimentales de la ley. Se aprueba por el Poder Ejecutivo o, cuando la ley lo habilite expresamente, por la propia autoridad de control, con plazos más breves de elaboración y modificación.

- Disposiciones y guías de la autoridad de control: orientaciones operativas, instrucciones sectoriales, recomendaciones de buenas prácticas. Su actualización es continua y no requiere procedimiento formal.

- Estándares técnicos de referencia: normas técnicas de seguridad, interoperabilidad y evaluación de conformidad, adoptadas por referencia a organismos de normalización reconocidos (ISO, NIST, ENISA, equivalentes nacionales).

El Salvador ilustra el funcionamiento de este tercer nivel. Los literales i) y n) del artículo 50 de la Ley para la Protección de Datos Personales facultan a la Agencia de Ciberseguridad del Estado (ACE) a elaborar y emitir políticas y guías, que complementan el marco legal sin requerir reforma legislativa.

5.2 Habilitaciones normativas delegadas

La ley debe prever habilitaciones explícitas a la autoridad de control para adoptar, mediante actos administrativos de alcance general, disposiciones vinculantes sobre materias técnicas específicas, como evaluaciones de impacto sectoriales o requisitos de seguridad por sector de actividad. Las habilitaciones que alcancen materias sustantivas -la ampliación de las categorías de datos sensibles, la modificación de clasificaciones de riesgo o la regulación de nuevos tipos de transferencias internacionales- requieren una habilitación legal expresa y quedan sujetas a los límites constitucionales de cada ordenamiento. En todos los casos, deben estar delimitadas en cuanto a su objeto, finalidad y procedimiento, y sujetas a los controles que prevea cada sistema jurídico.

5.3 Principio de neutralidad tecnológica

Las definiciones legales deben formularse en términos funcionales, no tecnológicos, para que sean aplicables a modalidades de tratamiento no conocidas en el momento de la sanción de la ley. La definición de 'datos personales', 'tratamiento', 'responsable' y 'sistema automatizado' debe ser lo suficientemente amplia para incluir las tecnologías emergentes sin requerir modificación legislativa.

5.4 Regulación basada en riesgos

El enfoque regulatorio basado en riesgos, aplicado de manera paradigmática por el RGPD europeo permite concentrar las obligaciones más intensas en los tratamientos que presentan mayores riesgos para los derechos fundamentales, y alivia la carga regulatoria sobre tratamientos de bajo riesgo. Este enfoque tiene la ventaja adicional de ser adaptable: a medida que evolucionan las tecnologías y sus riesgos son mejor comprendidos, la reclasificación del nivel de riesgo puede realizarse por vía reglamentaria sin necesidad de reforma legal, siempre que exista una habilitación legal expresa y dentro de los límites constitucionales de cada ordenamiento.

5.5 Sandbox regulatorio o entorno de prueba

Los entornos regulatorios experimentales, conocidos como regulatory sandboxes, constituyen un mecanismo innovador que permite a las autoridades de control y a los responsables del tratamiento explorar aplicaciones tecnológicas novedosas en un marco flexible pero supervisado. En Argentina, diversos proyectos legislativos han comenzado a incorporar esta herramienta como parte del debate sobre regulación de la innovación. En Brasil, la ANPD implementó el Sandbox Regulatorio de Inteligencia Artificial y Protección de Datos, que constituye la experiencia más avanzada de la región en esta materia.

En el plano comparado, el modelo británico, particularmente a partir de la experiencia de la Financial Conduct Authority, ha consolidado este enfoque como una de las principales estrategias de regulación pro-innovación.

La incorporación de habilitaciones legales para la creación de sandbox regulatorios en legislaciones de protección de datos permite generar aprendizaje empírico sobre riesgos específicos antes de regular de manera definitiva, y facilita la colaboración entre reguladores y desarrolladores tecnológicos.

6. Mecanismos de actualización periódica

Más allá del diseño normativo ágil, toda legislación de protección de datos debe contemplar mecanismos explícitos de revisión y actualización periódica que garanticen su vigencia sin depender de la iniciativa parlamentaria espontánea. Los mecanismos o componentes que constituyen propuestas de *lege ferenda* se identifican expresamente.

6.1 Cláusulas de revisión obligatoria

La ley debe establecer una obligación periódica de revisión integral de su contenido, con plazos definidos (por ejemplo, cada cinco años) y atribuida a un órgano específico (la autoridad de control, una comisión parlamentaria especializada o un consejo consultivo multisectorial). El resultado de cada revisión debe producirse en forma de informe público con recomendaciones de modificación o ratificación de los contenidos vigentes, independientemente de si se impulsa una reforma legislativa.

6.2 Informes anuales de la autoridad de control

La autoridad de control debe estar obligada a presentar anualmente al Parlamento un informe sobre el estado de la protección de datos en el país, que incluya: evaluación del cumplimiento de la legislación por sectores, análisis de las principales amenazas tecnológicas emergentes, propuestas de modificación normativa y recomendaciones de política pública. Este informe debe ser público y debe generar un debate parlamentario obligatorio, al menos en la comisión especializada (propuesta de lege ferenda).

6.3 Observatorio permanente de tecnologías emergentes (propuesta de lege ferenda)

El marco normativo debe prever la creación, o la asignación a la autoridad de control, de una función de observatorio permanente sobre las tendencias tecnológicas con impacto en la protección de datos personales. Esta función debe incluir la capacidad de emitir alertas tempranas, guías de evaluación de riesgos y recomendaciones sectoriales. A nivel regional, el **Observatorio Iberoamericano de Protección de Datos**, creado en el marco del XXII Encuentro de la RIPD, cumple esta función de manera complementaria a los observatorios nacionales.

6.4 Procedimiento acelerado de reforma parcial (propuesta de lege ferenda)

Para supuestos de urgencia regulatoria, tecnologías que plantean riesgos graves e inminentes para derechos fundamentales y que no están cubiertas por el marco vigente, la ley debe prever un procedimiento acelerado de reforma parcial, que reduzca los plazos del procedimiento legislativo ordinario sin comprometer la participación ciudadana mínima. Este mecanismo puede combinarse, cuando la ley lo prevea expresamente y dentro de los límites constitucionales de cada ordenamiento, con la habilitación a la autoridad de control para adoptar medidas cautelares de efecto inmediato mientras se tramita la reforma.

6.5 Participación multisectorial institucionalizada (propuesta de lege ferenda)

La experiencia de los procesos de reforma más exitosos, muestra que la participación amplia y estructurada de múltiples actores -academia, sociedad civil, sector privado, sector público, comunidades técnicas- es una condición de calidad y de legitimidad del resultado. Esta participación no debe ser episódica sino institucionalizada: la autoridad de control debe contar con un consejo consultivo permanente con representación multisectorial, cuya opinión sea preceptiva -aunque no vinculante- para las reformas normativas más relevantes.

El proceso de elaboración del Proyecto de Ley de Datos Personales argentino impulsado por la AAIP en 2023, con sus once mesas de diálogo y 173 aportes en consulta pública, es un ejemplo de buena práctica en esta dimensión, que requiere para su plena eficacia la institucionalización del mecanismo con carácter permanente, no solo en el momento de la reforma. Esa misma línea se tomó en la reforma de ese proyecto con 4 mesas multisectoriales para analizar una serie de temas específicos.

6.6 Cláusula de caducidad tecnológica (propuesta de lege ferenda)

Para disposiciones específicamente vinculadas a tecnologías o modalidades de tratamiento concretas -por ejemplo, regulaciones sobre sistemas de reconocimiento facial, identificación biométrica por voz, o modelos de lenguaje de IA generativa- la ley puede prever cláusulas de caducidad automática, que establezcan que esas disposiciones serán objeto de revisión específica en un plazo determinado (por ejemplo, tres años desde su entrada en vigor) y quedarán derogadas si no son ratificadas o actualizadas por el procedimiento correspondiente.

7. Recomendaciones

Las siguientes recomendaciones se dirigen a los procesos de reforma legislativa en curso en el espacio iberoamericano.

Para los legisladores nacionales

1. Priorizar la actualización de la legislación de protección de datos como paso previo a la regulación de la inteligencia artificial. La experiencia comparada demuestra que un marco sólido de protección de datos es la infraestructura legal indispensable para cualquier regulación efectiva de IA.

2. Adoptar una arquitectura normativa en capas que distinga entre la ley marco (estable), la reglamentación de desarrollo (flexible) y las disposiciones de la autoridad de control (continuas). Esta estructura permite agilidad sin sacrificar certeza jurídica.

3. Incorporar explícitamente la regulación de decisiones automatizadas e inteligencia artificial, incluyendo el derecho a la intervención humana y la obligación de evaluación de impacto algorítmico.

4. Garantizar y fortalecer la independencia de la autoridad de control, con autonomía funcional, orgánica y presupuestaria respecto del Poder Ejecutivo.

5. Prever mecanismos de revisión periódica obligatoria, al menos cada cinco años, con participación multisectorial institucionalizada.

6. Explorar la incorporación de habilitaciones legales para la creación de sandbox regulatorios en materia de protección de datos.

Para las autoridades de control

1. Ejercer activamente las habilitaciones normativas delegadas que la ley les confiera expresamente para actualizar por vía reglamentaria las disposiciones técnicas de la legislación vigente, dentro de los límites constitucionales de cada ordenamiento y sin esperar a reformas legislativas integrales.

2. Desarrollar y publicar guías sectoriales sobre el tratamiento de datos por tecnologías emergentes como sistemas de inteligencia artificial, con particular atención a los sectores salud, justicia, seguridad y servicios financieros.

3. Fortalecer la cooperación en el marco de la RIPD, incluyendo la adopción de las cláusulas contractuales modelo para transferencias internacionales y la participación activa en el proceso de actualización de los Estándares Iberoamericanos.

4. Establecer mecanismos de alerta temprana sobre tecnologías emergentes con impacto en la protección de datos, articulados con los mecanismos del Observatorio Iberoamericano.

Para la RIPD y sus instancias de coordinación regional

1. Desarrollar un modelo de ley tipo iberoamericana de protección de datos que sirva como referencia para los países de la región sin legislación vigente o con marcos significativamente desactualizados.

2. Establecer un mecanismo de monitoreo regional que evalúe periódicamente el grado de implementación efectiva de los estándares por parte de los países miembros, con publicación de informes periódicos.

3. Promover la adopción regional de las cláusulas contractuales modelo de la RIPD como instrumento prioritario para garantizar la protección de los flujos transfronterizos de datos.

8. Referencias

Instrumentos normativos internacionales y regionales

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo (RGPD). Diario Oficial de la Unión Europea, 4 de mayo de 2016.
- Estándares de Protección de Datos Personales para los Estados Iberoamericanos, Red Iberoamericana de Protección de Datos (RIPD), 2017 y 2026.
- Recomendación sobre la Ética de la Inteligencia Artificial, UNESCO, París, 23 de noviembre de 2021.
- Principios de la OCDE sobre Inteligencia Artificial, 2019 (actualizados 2024).
- Principios actualizados sobre la privacidad y la protección de datos personales, Organización de los Estados Americanos (OEA), 2021.
- Plan Estratégico 2026–2030 de la RIPD, aprobado en el XXII Encuentro Iberoamericano, Cartagena de Indias, 26 a 28 de mayo de 2025.
- Carta Iberoamericana de Principios y Derechos en los Entornos Digitales (CIPDED), SEGIB, 2023.

Legislación nacional analizada y citada

- Argentina: Ley 25.326 de Protección de Datos Personales (2000); Proyecto de Ley de Reforma AAIP – Mensaje 87/2023; Expediente 2130-D-2025 (Gollán); Expediente 3422-D-2024 (Yeza).
- Brasil: Lei 13.709/2018 – Lei Geral de Proteção de Dados (LGPD); Ley N° 15.352/2026, que transforma la ANPD en agencia reguladora; Ley N° 15.211/2025, Estatuto Digital del Niño y del Adolescente (ECA Digital); Decreto N° 12.975/2026, modificatorio del Marco Civil de Internet; Decreto N° 12.976/2026, sobre protección de las mujeres en entornos digitales.
- Chile: Ley 21.719 de Protección y Tratamiento de Datos Personales (promulgada diciembre 2024; vigencia diciembre 2026), originada en los boletines refundidos 11092-07 y 11144-07, ambos de 2017; Boletín 18623-07 (proyecto de modificación de la Ley 21.719, presentado el 1 de septiembre de 2026).

- Ecuador: Ley Orgánica de Protección de Datos Personales (LOPDP), publicada en el Quinto Suplemento del Registro Oficial Nº 459, de 26 de mayo de 2021; Reglamento General de la LOPDP (noviembre de 2023).

- Ecuador: Resolución Nº SPDP-SPD-2026-0009-R, Norma General para la Garantía del Derecho de Protección de Datos Personales en el Uso de Sistemas de Inteligencia Artificial, y su reforma por Resolución Nº SPDP-SPD-2026-0037-R; Resolución Nº SPDP-SPD-2026-0004-R, sobre cláusulas contractuales modelo de la RIPD; Resolución Nº SPDP-SPD-2025-0028-R, Reglamento del Delegado de Protección de Datos Personales.

- El Salvador: Ley para la Protección de Datos Personales (LPDP), artículo 50.

- México: Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (2025) y Ley Federal de Protección de Datos Personales en Posesión de Particulares (2025), que abrogan y sustituyen la legislación anterior. Decreto constitucional de simplificación orgánica, DOF 20 de diciembre de 2024.

- Uruguay: Ley 18.331 de Protección de Datos Personales y Acción de Habeas Data (2008); Ley 19.670 (reforma 2018); Decreto 64/020.

Documentos institucionales

- Agencia de Acceso a la Información Pública (AAIP). (2022). Informe sobre el Proceso de Elaboración Participativa de Normas. Buenos Aires: AAIP.

- AEPD / RIPD. (2025, junio). La Red Iberoamericana de Protección de Datos traza su hoja de ruta para los próximos años. Nota de prensa. Madrid.

- SEGIB / RIPD. (2024, noviembre). Acuerdo SEGIB-RIPD para avanzar en la protección de datos en la región. Madrid.

- García Balcarce, L. (2025). Discusión legislativa actual sobre Inteligencia Artificial en Argentina. Buenos Aires: documento de trabajo.

- Guilera, S., Pomares, J., Guillén, M. B., & Luvini, P. (2024). Marcos regulatorios de la IA: tendencias emergentes en la agenda legislativa argentina. Universidad Torcuato Di Tella, CEPE y GIDE.

- Derechos Digitales. (2025, enero). 2024: el año en que la protección de datos nos recordó su lado político. Santiago de Chile.

- R3D: Red en Defensa de los Derechos Digitales. (2024, diciembre). Réquiem por el INAI: un retroceso para la defensa de los derechos digitales. Ciudad de México.

- Garrigues Abogados. (2025). Las reformas en materia de protección de datos personales en Latinoamérica y sus efectos en las relaciones de trabajo. Madrid.