Gobernanza tecnológica adaptable: hacia políticas públicas flexibles para tecnologías disruptivas en América Latina y el Caribe

Gobernanza tecnológica adaptativa: Hacia políticas públicas flexibles para tecnologías disruptivas en América Latina y el Caribe

Magister Nicole Angel Sánchez Rojas

Las opiniones expresadas son responsabilidad exclusiva de la autora y no reflejan necesariamente la política o posición de LACNIC

Tabla de contenido

Resumen ejecutivo 3

Glosario/Acrónimos 4

1. Introducción 5

2. Revisión de literatura / Marco conceptual y teórico 6

2.1 Tecnologías disruptivas: definición y evolución 7

2.1. Gobernanza tecnológica adaptable: principios y marcos de referencia 8

2.2. Modelos regulatorios comparativos: entre el derecho blando y el derecho duro 9

2.3. Desigualdades estructurales, brechas digitales y la perspectiva del Sur Global 10

2.4. Adopción de políticas de IA en América Latina 10

2.5. Estado de la protección de datos 11

2.6. Panorama de la ciberseguridad y la ciberdelincuencia 12

2.7. Marco institucional y capacidades regulatorias 13

2.9 Grado de anticipación y resiliencia regulatoria y participación y representación de múltiples partes interesadas 13

3. Metodología 14

3.1 Desafíos comunes: obsolescencia, fragmentación y falta de interoperabilidad 14

3.1. Justificación del enfoque cualitativo 15

3.2. Selección de participantes para las entrevistas 15

3.3. Consentimiento, anonimato 15

3.4. Formatos de entrevistas y reflexividad del investigador 16

4. Análisis/Mapeo de buenas prácticas y modelos flexibles/ Entrevistas con profesionales regionales 16

4.1. Experiencias internacionales y regionales de gobernanza adaptativa 16

4.2 Casos exitosos de co-creación y regulación basada en principios 17

4.3 Mecanismos de gobernanza distribuida y regulación en evolución 18

Mapeo comparativo de la normativa sobre IA, protección de datos y ciberdelitos en Argentina, Bolivia, Brasil, Chile, Colombia, República Dominicana y México 19

4.4. Entrevistas y análisis participativo: análisis clave esperado 24

Perspectivas de las partes interesadas y mapeo de la preparación legal en materia de protección de datos, inteligencia artificial y regulación de los delitos cibernéticos: Resultados de entrevistas en siete países de América Latina y el Caribe 25

5. Hallazgo 39

6. Conclusiones y recomendaciones 43

Referencias bibliográficas 45

Apéndice 47

Resumen ejecutivo

América Latina y el Caribe se encuentran hoy en un punto de inflexión decisivo. La rápida expansión de la inteligencia artificial, las plataformas digitales y los desafíos de la ciberseguridad han abierto oportunidades para la innovación, pero también han expuesto marcos legales frágiles y profundas brechas institucionales. Mientras Europa se prepara para la entrada en vigencia del AI Act y América del Norte identifica con evaluaciones de impacto de los algoritmos, muchos países de la región siguen atrapados entre modelos importados y las realidades apremiantes de la desigualdad, la falta de normativas eficaces y la dependencia tecnológica. Esta investigación demuestra que la gobernanza de las tecnologías disruptivas en el Sur Global no puede ser una simple imitación, debe adaptarse en los contextos locales, inspirarse en las voces regionales y diseñarse como una estrategia de supervivencia en entornos volátiles y desiguales.

A partir de un estudio normativo comparado de Argentina, Bolivia, Brasil, Chile, Colombia, República Dominicana y México, complementado con entrevistas a expertos, este trabajo revela una persistente desconexión entre las promesas de la regulación y sus efectos concretos. Países como Brasil y Chile ilustran avances importantes a través de la LGPD y una ley integral de ciberseguridad, mientras que otros, como Bolivia y República Dominicana, operan con marcos incompletos u obsoletos que exponen a poblaciones enteras. En los distintos casos, tres elementos emergen con particular claridad, primero, que la dependencia normativa de los modelos europeos genera cargas de cumplimiento desconectadas de la capacidad local; segundo, que la fragilidad institucional y la escasez de recursos son una brecha de credibilidad de las autoridades reguladoras; y tercero, que la falta de conciencia pública reduce las protecciones a garantías simbólicas en lugar de derechos efectivos.

Al mismo tiempo, el estudio destaca cómo las voces regionales convergen en una urgencia común, construir modelos de gobernanza que prioricen los derechos, la equidad y la participación. La evidencia demuestra que las leyes no pueden simplemente regular la tecnología como un objeto externo; deben incorporar mecanismos de rendición de cuentas, transparencia e inclusión capaces de anticipar riesgos y corregir desigualdades. Las autoridades independientes y dotadas de recursos, la conciencia ciudadana y la alfabetización digital, así como la coordinación regional más allá de las declaraciones retóricas no son ambiciones secundarias, sino pilares fundamentales. Sin ellas, la transición digital seguirá siendo ambiciosa y excluyente, amplificando las mismas desigualdades que promete superar.

La conclusión es inevitable, América Latina y el Caribe se enfrenta a una encrucijada en la que dos futuros divergen. Uno está marcado por la dependencia, la fragmentación y la reproducción de la desigualdad bajo la fachada de leyes modernas. El otro prevé una gobernanza adaptativa, participativa y contextualizada, capaz de transformar las tecnologías disruptivas en herramientas para la democracia, la justicia social y el desarrollo sostenible. La decisión está en manos de los gobiernos, las instituciones y las sociedades de la región, pero la dirección es clara, los derechos no deben añadirse a posteriori, sino que deben constituir la base de la gobernanza misma. Solo así la transformación digital podrá convertirse, no en una nueva capa de desigualdad, sino más bien, en la arquitectura de un futuro más digno y equitativo.

Glosario/Acrónimos

- **Gobernanza Adaptativa:** Modelo regulatorio que se ajusta dinámicamente al cambio tecnológico mediante revisión, evaluación de riesgos y participación multisectorial.
- **IA (Inteligencia Artificial):** Sistemas capaces de aprender, razonar y tomar decisiones a partir de datos, incluidos modelos generativos.

- **ANPD (Autoridade Nacional de Proteção de Dados):** la autoridad nacional de protección de datos de Brasil, creada para supervisar la implementación y el cumplimiento de la LGPD.
- **Convenio de Budapest:** Tratado del Consejo de Europa sobre la ciberdelincuencia, que sirve como principal estándar internacional para la cooperación en materia de derecho penal digital.
- **Delito cibernético:** Actividad delictiva realizada a través de tecnologías digitales, como ransomware, robo de identidad o ciberviolencia.
- **Ciberseguridad:** Protección de redes, sistemas y datos contra accesos no autorizados, ataques o interrupciones para garantizar la resiliencia.
- **Protección de Datos (PD):** Garantías legales que regulan el tratamiento de datos personales, garantizando la privacidad, la dignidad y el control sobre la información.
- **DPO (Delegado de Protección de Datos):** Rol designado y obligatorio en algunos regímenes (por ejemplo, GDPR, LGPD) para supervisar el cumplimiento de la ley de protección de datos.
- **Brecha digital** : desigualdad estructural en el acceso a Internet, dispositivos y habilidades digitales, que a menudo afecta a grupos rurales y marginados.
- **GIRAI (Índice Global de IA Responsable):** Referencia internacional que mide la adopción de IA responsable, incluyendo dimensiones de género y derechos humanos.
- **Perspectiva del Sur Global:** Lente analítica que enfatiza la gobernanza contextualizada adaptada a las realidades sociopolíticas y económicas de América Latina.
- **RGPD (Reglamento General de Protección de Datos):** Reglamento de la Unión Europea que establece estrictas protecciones de datos personales, ampliamente referenciado a nivel mundial.
- **ILIA (Índice Latinoamericano de Inteligencia Artificial):** Índice regional que mide la preparación, adopción y gobernanza de la IA en los países de América Latina.
- **LGPD (Ley General de Protección de Dados):** Ley general de protección de datos de Brasil (2018/2020) inspirada en el RGPD pero adaptada a las realidades nacionales.
- **Dependencia normativa:** Dependencia de modelos regulatorios externos sin adaptación, lo que resulta en marcos ineficaces o simbólicos.
- **OEA (Organización de los Estados Americanos):** Organismo regional que promueve la cooperación en ciberseguridad, gobernanza digital y derechos humanos en las Américas.
- **OCDE (Organización para la Cooperación y el Desarrollo Económicos):** organismo internacional que emite directrices sobre IA y gobernanza digital adoptadas como referencias de derecho indicativo.
- **Regulación basada en principios:** modelo regulatorio flexible basado en valores amplios (transparencia, rendición de cuentas, no discriminación) en lugar de reglas prescriptivas.
- **Ética de la IA de la UNESCO:** primer instrumento normativo mundial (2021) que establece principios para el desarrollo y la implementación éticos de la IA.
- **Objetivos de Desarrollo Sostenible (ODS) de la ONU:** Agenda global que vincula la innovación tecnológica con objetivos de equidad, sostenibilidad y derechos humanos.

1. Introducción

Vivimos en la era de la convergencia tecnológica, donde el ritmo acelerado del big data, la digitalización, la inteligencia artificial (IA), blockchain y en los años siguientes la computación cuántica emergente, van ejerciendo presión sobre la capacidad regulatoria en todos los países del mundo, pero los países de América Latina y el Caribe enfrentan algunos desafíos adicionales.

Uno de los principales desafíos en América Latina, es la tendencia a importar modelos regulatorios europeos sin adaptarlos a las realidades sociopolíticas regionales. Un caso que podemos analizar es la experiencia brasileña, que muestra que, si bien el Senado aprobó un proyecto de ley en 2024 inspirado en la Ley de IA de la UE, su avance ha sido lento y desigual. El texto propone clasificar los sistemas según su nivel de riesgo y exige evaluaciones de impacto, pero se basa en la premisa de que no debe haber un equilibrio entre la protección de los derechos y el desarrollo económico. Al mismo tiempo, las investigaciones revelan que el sector privado dominó un tercio de las audiencias legislativas, mientras que la academia y la sociedad civil participaron mucho menos. Esta asimetría subraya la necesidad de modelos participativos y adaptados localmente, ya que replicar normas extranjeras sin una amplia inclusión puede reproducir sesgos y no abordar las brechas estructurales de la región. Esto es algo que ocurre constantemente en la región, en el intento de alcanzar estándares internacionales, pero olvidando la realidad nacional.

En este contexto, la presente investigación no solo analizará los marcos normativos y los documentos de política de cada país seleccionado, sino que también incorporará entrevistas semiestructuradas con profesionales legales, técnicos y de políticas públicas de toda la región. Esta metodología mixta busca captar conocimiento del entorno y diversas perspectivas sobre el desarrollo y la implementación de la gobernanza de la IA, la protección de datos, la ciberdelincuencia, así como de otras tecnologías disruptivas. A través de estas entrevistas, el estudio busca ir más allá de los textos legales formales e identificar cómo las prioridades nacionales, las capacidades institucionales y las dinámicas sociopolíticas están moldeando o limitando el surgimiento de enfoques regulatorios adaptativos en América Latina y el Caribe.

Un estudio de CEPAL realizado en 2024 reveló que aproximadamente el 55% de personas encuestadas en Argentina, Brasil, Colombia y México apoyaba la regulación de la inteligencia artificial (IA). Sin embargo, el 37% expresó su preocupación por la posibilidad de que la IA exacerbara las desigualdades sociales. Algunos participantes también temían el uso de la IA en la toma de decisiones judiciales, mientras que un grupo considerable rechazaba la idea de implementar marcos regulatorios en esta etapa temprana del desarrollo tecnológico. Según estos encuestados, una regulación prematura podría vulnerar derechos fundamentales y facilitar el uso instrumental de la IA por parte de los gobiernos.

Un marco regulatorio obsoleto o inexistente deja a la población sin herramientas para proteger su privacidad y amplía la brecha digital en regiones con alta desigualdad, como Bolivia, Paraguay o Venezuela. La mención de estos países se debe a la falta de regulación en materia de derechos digitales y a que son los únicos tres países de América Latina que no cuentan con una normativa específica de protección de datos. Por estas razones, investigar mecanismos de gobernanza tecnológica adaptables es crucial para anticipar riesgos y salvaguardar los derechos fundamentales sin frenar la innovación.

Esta investigación adoptará un enfoque mixto que combina análisis documental, trabajo de campo y procesos participativos. Sobre esta base, el estudio se despliega en seis capítulos que trazan un recorrido desde el contexto hasta la acción. Los capítulos iniciales marcan el escenario, la introducción plantea el problema de investigación, mientras que la revisión de literatura ofrece las herramientas conceptuales para comprender las tecnologías disruptivas y los dilemas de gobernanza que generan. Posteriormente, la metodología explica cómo la investigación va más allá de los textos para capturar las realidades vividas por profesionales de toda la región.

El núcleo del trabajo se encuentra en el análisis, donde se mapean buenas prácticas y modelos innovadores, contrastados con las voces de expertos regionales. Estas miradas convergen en los hallazgos, que ponen en evidencia tanto las oportunidades como las fracturas que moldean el futuro digital de América Latina. Finalmente, el último capítulo reúne el camino recorrido en las

conclusiones y recomendaciones, no como simples prescripciones abstractas, sino como un llamado a la acción para construir una gobernanza tecnológica adaptable y centrada en los derechos, que dialogue con las realidades y aspiraciones propias de la región.

2. Revisión de literatura / Marco conceptual y teórico

En primer lugar, se realizará un estudio comparativo de los marcos legales y las políticas públicas sobre Inteligencia Artificial, Ciberdelitos y Protección de Datos en siete países de América Latina y el Caribe. Este análisis cubrirá las estructuras legales, su validez y sus brechas, evaluando si los textos se han adaptado al entorno local o se han copiado de modelos extranjeros. Se utilizarán matrices de países y tablas comparativas para sistematizar la información, y el Índice ILIA, que destaca que Chile, Brasil y Uruguay lideran la región en la adopción de IA (Chile 73,07 / Brasil 69,30 / Uruguay 64,98), servirá como referencia. ILIA también muestra que Argentina, Colombia y México se encuentran en la categoría de "adoptantes", con puntuaciones de preparación de nivel medio (CEPAL 2024), [1]y también servirá como referencia el GIRAI, un documento desarrollado con la cooperación de ILDA (Iniciativa Latinoamericana de Datos Abiertos), donde analizan cómo se está desarrollando la IA en diferentes países del mundo.

En segundo lugar, se desarrollará un diagnóstico cualitativo mediante entrevistas semiestructuradas y grupos focales con actores clave: formuladores de políticas, líderes del sector privado, la academia, activistas de derechos digitales y organizaciones internacionales. Estas entrevistas explorarán las percepciones de las brechas, las prioridades regulatorias y los obstáculos para la regulación adaptativa. Como se encontró en los casos de EmpatIA /ILDA, los proyectos de coproducción revelaron que la inclusión de comunidades no tradicionales, la transparencia, la transferencia de conocimiento y la calidad de los datos son esenciales para la legitimidad y el impacto [2]. Finalmente, se construirá un mapeo de las mejores prácticas identificando casos de gobernanza flexible (por ejemplo, regulaciones basadas en principios, entornos regulatorios de prueba o mecanismos de co-creación) y evaluando su replicabilidad. El proyecto concluirá con recomendaciones de políticas y puntos de mejora para la región.

El estudio incluirá un análisis regional de siete países de América Latina y el Caribe: Argentina, Bolivia, Brasil, Chile, Colombia, República Dominicana y México. Esta selección permite analizar diversos enfoques legales e institucionales para la gobernanza de tecnologías disruptivas, como la inteligencia artificial, la protección de datos y la ciberdelincuencia. Algunos de estos países han adoptado marcos regulatorios o estrategias nacionales en estas áreas, mientras que otros aún carecen de normas coherentes o aplicables y enfrentan la necesidad de una profunda reestructuración legal e institucional.

La investigación examinará tanto la existencia como la eficacia de los mecanismos de gobernanza actuales, identificando brechas regulatorias, debilidades institucionales y riesgos de obsolescencia normativa. También explorará prácticas que, si bien no están necesariamente consolidadas, ofrecen perspectivas relevantes para una gobernanza participativa y adaptativa. A través de este análisis comparativo, el estudio busca extraer lecciones y recomendaciones concretas para el diseño de políticas públicas más receptivas e inclusivas en la región, basadas en las realidades locales y capaces de abordar el rápido cambio tecnológico.

---

[1]Comisión Económica de las Naciones Unidas para América Latina y el Caribe (CEPAL) y Centro Nacional de Inteligencia Artificial (CENIA). (2024). ILIA 2024: Evaluación de la preparación y el progreso de la IA en América Latina.
https://www.cepal.org/en/notes/ilia-2024-evaluating-ai-readiness-and-progress-latin-america

[2]Iniciativa Latinoamericana de Datos Abiertos (ILDA). EmpatIA : IA para resolver problemas públicos en Latinoamérica. (2022-23). Descripción del proyecto EmpatIA y resúmenes de políticas. ILDA. Foro de París sobre la Paz.

2.1 Tecnologías disruptivas: definición y evolución

Las tecnologías disruptivas son innovaciones que transforman radicalmente los modelos de negocio, las estructuras sociales y la dinámica del mercado. En el contexto de este estudio, el enfoque se centra principalmente en la inteligencia artificial (IA), la protección de datos y sus consecuencias, como la ciberdelincuencia. La IA abarca sistemas capaces de aprender y tomar decisiones basadas en datos masivos, su evolución reciente incluye el aprendizaje profundo y los modelos generativos que pueden crear texto, imágenes y código. El análisis de otras tecnologías, como el big data, se refiere al procesamiento de grandes volúmenes de datos procedentes de dispositivos móviles, sensores, redes sociales y transacciones digitales, cuyo análisis revela patrones y predice comportamientos. Sin embargo, existen otros desafíos que debemos empezar a considerar, como la computación cuántica, que utiliza cúbits para procesar información mediante superposición y entrelazamiento, que promete resolver problemas complejos inmanejables por la computación clásica. En conjunto, estas tecnologías prometen optimizar procesos y crear valor, pero también aumentan riesgos como la discriminación algorítmica, los monopolios de datos y las vulnerabilidades de seguridad.

La adopción y evolución de tecnologías disruptivas en América Latina y el Caribe se caracterizan por fuertes asimetrías. Si bien la proliferación de dispositivos conectados y la mayor disponibilidad de datos han acelerado la experimentación con inteligencia artificial, blockchain y otras tecnologías emergentes, las persistentes brechas en infraestructura, habilidades digitales e inversión en investigación y desarrollo limitan su implementación más amplia. El Índice Latinoamericano de Inteligencia Artificial (ILIA, 2024) identifica a Chile (73,07), Brasil (69,30) y Uruguay (64,98) como pioneros, destacando el progreso en las estructuras de gobernanza, los ecosistemas de I+D (Investigación y Desarrollo) y la infraestructura digital, junto con las iniciativas de los sectores público y privado destinadas a fomentar la innovación.

Al mismo tiempo, países como Argentina (55,77), Colombia (52,64) y México (51,40) se clasifican como "adoptadores", lo que refleja avances parciales en el despliegue de IA y la preparación institucional, pero aún enfrentan desafíos estructurales como la coordinación limitada entre sectores, la fragmentación regulatoria y la escasez de apoyo al talento [3]. A pesar de que la región duplicó su participación en el talento relacionado con IA en los últimos ocho años, ningún país ha alcanzado los niveles observados en el Norte Global. Además, la baja inversión pública en ciencia y tecnología, el acceso desigual a Internet y los sistemas educativos frágiles continúan limitando la escalabilidad de las tecnologías avanzadas, incluida la computación cuántica [4]. Cualquier diseño regulatorio o de políticas debe considerar estas asimetrías para evitar profundizar las desigualdades existentes y garantizar que la innovación contribuya al desarrollo inclusivo y sostenible.

2.1. Gobernanza tecnológica adaptable: principios y marcos de referencia

La gobernanza tecnológica adaptable se define como un conjunto de mecanismos regulatorios capaces de anticipar, absorber y responder a la evolución de las tecnologías disruptivas. A diferencia de la regulación estática, la gobernanza adaptable combina enfoques basados en el

---

[3]Comisión Económica para América Latina y el Caribe (CEPAL). (24 de septiembre de 2024). El Índice Latinoamericano de Inteligencia Artificial (ILIA) reconfirma a Chile, Brasil y Uruguay como líderes de la región. CEPAL. https://www.cepal.org/es/comunicados/de-prensa/el-indice-latinoamericano-de-inteligencia-artificial-ilia-confirma-a-chile-brasil-y-uruguay

[4]Levy Yeyati , E. (22 de mayo de 2025). Estrategias de regulación inteligente de la IA para los responsables de políticas públicas en América Latina. Brookings Institution. https://www.brookings.edu/articles/smart-ai-regulation-strategies-for-latin-american-policymakers/

riesgo, la revisión periódica y la participación multisectorial. El informe de Brookings sobre la regulación inteligente de la IA identifica cinco prioridades para América Latina:

1. Facilitar la innovación mediante entornos regulatorios que reduzcan la incertidumbre.
2. Promover la inclusión mediante la inversión en alfabetización digital y herramientas de código abierto.
3. Institucionalizar la seguridad a través de institutos nacionales o regionales de seguridad de la IA;
4. Prevenir la monopolización aligerando las cargas regulatorias para las PYME y promoviendo la neutralidad competitiva;
5. Impulsar la armonización regional mediante estándares de datos compartidos y marcos transfronterizos.

Estos principios requieren una regulación flexible, interactiva y actualizable que sea vista no como un mero control sino como una estrategia de desarrollo inclusiva.

Europa puede ser un ejemplo de cómo los países pueden trabajar en una regulación regional, América Latina y el Caribe pueden tomar como ejemplo el trabajo conjunto regional. Trabajar en la armonización regional de los marcos regulatorios podría ser un camino a seguir para lograr la cooperación internacional en la defensa de los derechos humanos y al mismo tiempo, apoyar la innovación en la región.

A nivel internacional, la Ley de IA de la UE ha promovido modelos basados en el riesgo que prohíben sistemas inaceptables y exigen evaluaciones de impacto para sistemas de alto riesgo. Access Now advierte que muchos proyectos de ley latinoamericanos replican estos enfoques, clasificando los sistemas por nivel de riesgo y analizando las estrategias nacionales para comprender sus objetivos y métodos. Sin embargo, un modelo adaptativo debería basarse en estándares globales (como las directrices éticas de IA de la UNESCO o la Recomendación de la OCDE), adaptándolos a la capacidad regulatoria y las necesidades sociales de cada país. Una gobernanza adaptable también implica transparencia algorítmica, rendición de cuentas y mecanismos para la actualización regulatoria y la colaboración transfronteriza.

2.2. Modelos regulatorios comparativos: entre el derecho blando y el derecho duro

El debate entre el derecho indicativo y el derecho imperativo para las tecnologías disruptivas se centra en equilibrar la flexibilidad y la exigibilidad. El derecho indicativo abarca códigos de conducta, directrices éticas y declaraciones de principios que guían sin ser jurídicamente vinculantes, mientras que el derecho imperativo implica estatutos y reglamentos con obligaciones y sanciones. América Latina exhibe ambos enfoques. La mayoría de los países aún carecen de marcos específicos de IA y dependen de leyes de protección de datos existentes o estrategias nacionales no vinculantes, algunos países aún están en camino de regulaciones como la ley de protección de datos o la sanción de los ciberdelitos. Xenoss[5] señala que, aparte de Brasil, la mayoría de los países aún no han establecido marcos formales de gobernanza de la IA, muchos están redactando estrategias o permanecen inactivos. En consecuencia, los esfuerzos regulatorios están fragmentados y se centran en sectores como las finanzas, la salud o los servicios públicos, mientras que los marcos generales siguen ausentes.

Brasil, sin embargo, se destaca por proponer el primer proyecto de ley de IA de la región, el Proyecto de Ley n.º 2338/2023, inspirado en la Ley de IA de la UE. Este proyecto de ley categoriza los sistemas por riesgo (inaceptable, alto y bajo) e impone obligaciones

[5] Xenoss. (2023, October 27). AI regulation in Latin America (LATAM): Brazil leads. Xenoss Blog. https://xenoss.io/blog/latin-america-latam-ai-regulations

proporcionales, prohíbe los sistemas de riesgo excesivo, como la puntuación social y la vigilancia biométrica masiva, y exige transparencia, supervisión humana y mecanismos de remediación para los sistemas de alto riesgo [6].

Una perspectiva del Sur Global exige considerar la diversidad cultural, la soberanía digital y la justicia distributiva, promover la participación de las comunidades indígenas, afrodescendientes, así como femeninas, y prevenir la fuga de talento hacia los países desarrollados. También exige cuestionar la dependencia tecnológica y fomentar la innovación adaptada localmente en lugar de replicar modelos impuestos.

2.3. Desigualdades estructurales, brechas digitales y la perspectiva del Sur Global

Las desigualdades estructurales en la región impactan la adopción de IA, la aplicación de la protección de datos y la capacidad para combatir el cibercrimen. El Índice Latinoamericano de Inteligencia Artificial (ILIA 2024) destaca un mayor talento en IA, pero persisten brechas en infraestructura, conectividad y potencia computacional. Chile lidera con 73,07 puntos, Brasil con 69,30 y Uruguay con 64,98 sobre 100. Sin embargo, muchos otros países de la región presentan un rezago significativo en factores facilitadores y marcos de gobernanza [7].

El Índice Global de IA Responsable subraya las brechas globales: si bien el 39 % de los países encuestados cuenta con estrategias de IA, la mayoría carece de principios de IA responsable aplicables. Solo 24 países cuentan con marcos gubernamentales que abordan la cuestión del género y la IA [8]. Esto resuena en la región, donde varios entrevistados señalaron que los textos legales a menudo no incorporan políticas inclusivas de género ni mecanismos concretos de rendición de cuentas. Estas deficiencias afectan la aplicación de las leyes de datos y las medidas de ciberseguridad. Sin suficientes recursos, infraestructura técnica y capacitación, las autoridades no pueden supervisar ni aplicar las leyes eficazmente.

Entre el 22 y el 24 de julio, en el evento regional AbreLatam que se realizó en Bolivia, tuvimos diferentes espacios para discutir estas problemáticas (Datos, desigualdades e IA) que afectan a toda la región y en uno de los talleres desarrollados por Derechos Digitales e ILDA analizamos los riesgos relacionados con la IA y género con un enfoque importante en las desigualdades que podemos enfrentar cuando la tecnología no sigue un proceso preciso de rendición de cuentas, pero al mismo tiempo algunos de los participantes mencionaron que tal vez el problema en América Latina no es la tecnología, el problema real es el acceso limitado a internet y esa es una de las principales brechas en los países de América Latina y el Caribe.

En el mismo evento, algunos de los participantes mencionaron que el segundo problema que enfrentamos en Latino América, es la falta de conocimiento sobre el uso correcto de la tecnología, por lo que todos estos comentarios de miembros de diferentes países muestran algo nuevamente… el contexto y los problemas en la región no son los mismos que en Europa, por lo cual se deben desarrollar políticas públicas específicas enfocadas en el contexto de cada país.

---

[6] Panorama general de las políticas de IA en 10 jurisdicciones | Observatorio Digital Watch. (23 de diciembre de 2024). Observatorio Digital Watch. https://dig.watch/updates/overview-of-ai-policy-in-10-jurisdictions

[7] ILIA 2024: Evaluación de la preparación y el progreso de la IA en América Latina | CEPAL. (2024). Comisión Económica para América Latina y el Caribe. https://www.cepal.org/en/notes/ilia-2024-evaluating-ai-readiness-and-progress-latin-america

[8] La gobernanza de la IA no cumple con sus objetivos: el Índice Global de IA Responsable revela deficiencias críticas. (2024). Globalcenter.ai. https://www.globalcenter.ai/news/ai-governance-fails-to-deliver-global-index-on-responsible-ai-reveals-critical-gaps

Un enfoque del Sur Global requiere una regulación contextualizada e independencia normativa. Las tecnologías deben atender las necesidades locales y respetar la diversidad cultural, la soberanía digital y la justicia distributiva. Esto implica incluir a las comunidades indígenas, afrodescendientes y rurales en la formulación de políticas, promover la participación de las mujeres en la I+D y evitar el colonialismo digital. La cooperación regional también es crucial, especialmente en materia de ciberdelincuencia, donde la coordinación transnacional es necesaria.

2.4. Adopción de políticas de IA en América Latina

La adopción de políticas de IA en América Latina es muy desigual. ILIA 2024 clasifica a Chile, Brasil y Uruguay como "pioneros" debido a sus estrategias nacionales, inversión en infraestructura digital y el establecimiento de mecanismos de gobernanza. Estos países han desarrollado planes a largo plazo, alianzas público-privadas, así como programas de desarrollo de talento [9]. México, Argentina y Colombia se clasifican como "adoptantes", habiendo avanzado en investigación y desarrollo, pero aun enfrentando desafíos de gobernanza. Otros estados apenas están comenzando a explorar iniciativas o carecen de marcos regulatorios claros. Según la "Radiografía Regulatoria" de Access Now, existen múltiples proyectos de ley relacionados con la IA en discusión en Argentina, Chile, Colombia y México, pero la mayoría replican modelos europeos y carecen de una participación significativa de la sociedad civil.

México no cuenta con una regulación específica relacionada con Inteligencia Artificial pero sí ha implementado en algunos estados regulaciones para sancionar el uso de IA para desarrollar violencia digital, como la creación de imágenes o videos con fines sexuales utilizando el rostro de una persona. Brasil es el único país que ha impulsado un proyecto de ley de IA inspirado en la Ley de IA de la UE. La propuesta clasifica los sistemas de IA por nivel de riesgo y prohíbe aquellos considerados de riesgo inaceptable, como la puntuación social. Exige transparencia, supervisión humana y mecanismos de reparación para los sistemas de alto riesgo. Colombia, México y Argentina se encuentran debatiendo estrategias nacionales, pero aún se basan principalmente en leyes de protección de datos y directrices éticas no vinculantes. Estos enfoques reflejan una transición del derecho indicativo a marcos híbridos, sin embargo, su implementación efectiva depende de la capacidad institucional y la coordinación interinstitucional.

2.5. Estado de la protección de datos

Los regímenes de protección de datos en la región son diversos. En la década de los 90, diferentes países iniciaron el proceso de implementación de regulaciones sobre protección de datos. Dos de los primeros países fueron Argentina y Chile, pero con el tiempo Uruguay y Brasil mostraron grandes avances, como, por ejemplo, los parámetros del RGPD (Reglamento General de Protección de Datos). Países como Colombia o Ecuador tardaron más en implementar la regulación, pero también la implementaron.

Brasil implementó la LGPD [10]en 2020, desde 2022, ha promovido cláusulas contractuales tipo y sanciones más estrictas. Argentina actualizó su legislación en 2024 para aumentar las multas y actualmente está actualizando sus estándares en temas de protección de datos y regulación de entornos digitales. México cuenta con una ley de protección de datos desde 2010, pero necesita

---

[9]Comisión Económica para América Latina y el Caribe y Centro Nacional de Inteligencia Artificial (CENIA). (7 de octubre de 2024). Índice Latinoamericano de Inteligencia Artificial (ILIA 2024): Evaluación de la preparación y el progreso de la IA en América Latina. https://www.cepal.org/en/notes/ilia-2024-evaluating-ai-readiness-and-progress-latin-america

[10]DLA Piper. (2024). Leyes de protección de datos en Brasil — En vigor desde el 18 de septiembre de 2020, la Ley General de Protección de Datos (LGPD) de Brasil. https://www.dlapiperdataprotection.com/index.html?c=BR&t=law

actualizaciones para regular nuevas tecnologías como la IA. En 2024, Chile aprobó un nuevo proyecto de ley de protección de datos, la cual entrará en plena vigencia en 2026 [11], que introduce los derechos ARCO, las obligaciones de notificación de incidentes y la figura del Delegado de Protección de Datos. Perú emitió un nuevo reglamento de privacidad (DS 016-2024-JUS), vigente desde marzo de 2025, que exige que los trabajadores sean informados sobre el procesamiento de datos personales e introduce la figura del Delegado de Protección de Datos con responsabilidades internas y externas.

Sin embargo, otros países de América Latina, como Bolivia, Paraguay y Venezuela, carecen de leyes específicas u operan con marcos regulatorios insuficientes [12]. A principios de 2025, Paraguay inició un debate sobre una regulación relacionada con la protección de datos, por otro lado, Bolivia no ha avanzado desde 2023. En 2024, se tuvo una reunión entre sociedad civil y la Agencia Gubernamental de Tecnologías de la Comunicación y la Información (AGETIC), que reconoció la necesidad de la ley, pero no una urgencia por parte del gobierno para aprobarla. Venezuela mantiene disposiciones parciales en materia de telecomunicaciones y derecho constitucional, pero carece de una legislación integral.

La disparidad regulatoria obstaculiza la cooperación transfronteriza y aumenta el riesgo de transferencias de datos sin garantías. Las empresas deben navegar por un complejo mosaico regulatorio, lo que dificulta el cumplimiento y desalienta la inversión. Este contexto exige la armonización regional y el fortalecimiento de autoridades de protección de datos independientes y con recursos suficientes.

Algunos países de la región como Chile [13]y Perú están desarrollando algunas actualizaciones en su regulación de Protección de Datos, con el objetivo de desarrollar medidas de ciberseguridad y legislación de Inteligencia Artificial.

2.6. Panorama de la ciberseguridad y la ciberdelincuencia

La región muestra un vacío regulatorio general en materia de ciberdelincuencia. Uno de los ejemplos más recientes que podemos analizar es Chile, que destaca por su Ley de Ciberseguridad [14], aprobada en 2023 y vigente desde enero de 2025. La ley crea la ANCI (Agencia Nacional de Ciberseguridad), la cual obliga a los proveedores de servicios esenciales a implementar medidas de seguridad y reportar incidentes al Equipo Nacional de Respuesta a Incidentes de Seguridad Informática y establece un Consejo Multisectorial con participación de la sociedad civil y la academia. Designa a los sectores críticos (salud, energía, banca, telecomunicaciones) sujetos a la ley y establece sanciones por incumplimiento.

Brasil incluye disposiciones sobre ciberdelitos en su Código Penal y cuenta con una estrategia de ciberseguridad, pero carece de una ley integral. México cuenta con una Estrategia Nacional de Ciberseguridad, programática y no vinculante, sin embargo, esta se vio afectada en los últimos meses tras la decisión de cerrar el INAI y un cambio en la estrategia nacional, acciones que, una vez más, exigen al país la reflexión sobre nuevas estrategias.

---

[11]Nueva Ley de Protección de Datos de Chile: Contexto, Panorama y Conclusiones Clave. (27 de febrero de 2025). FPF. https://fpf.org/blog/chiles-new-data-protection-law-context-overview-and-key-takeaways

[12]Privacidad de datos en América Latina. (28 de enero de 2025). Crowell & Moring: Informes nacionales sobre protección de datos. https://www.crowell.com/en/insights/publications/latin-american-data-privacy

[13]Chile – Leyes de Protección de Datos y Ciberseguridad. (2025). Guía de Expertos de CMS. https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/chile?format=pdf&v=3

[14] Fortra . (27 de julio de 2025). Panorama regulatorio de la ciberseguridad en Chile: Guía para empresas. https://www.fortra.com/blog/cybersecurity-regulatory-landscape-chile-primer-businesses

Colombia y Argentina cuentan con normas dispersas en sus códigos penales, mientras que países como Bolivia y Paraguay carecen de una tipificación clara de delitos como el ransomware o los ataques a infraestructuras críticas, en el caso de Bolivia se cuenta con solamente dos articulados en el código penal, la manipulación informática y alteración, acceso y uso indebido de datos informáticos, los cuales no se abarcan todos los delitos en entornos virtuales que existen hoy en día[15]. La ausencia de marcos integrales dificulta el procesamiento penal, la cooperación internacional, la protección de infraestructuras críticas y la defensa de los derechos digitales. Estudios regionales como el de América Latina y el Caribe, "Escalando la Escalera de la Ciberseguridad" [16] muestran que varios países han desarrollado marcos legales para combatir el ciberdelito, pero muchos aún se encuentran en etapas inmaduras en su aplicación procesal.

Pero una vez más, la solución no es sólo copiar una regulación europea, necesitamos construir una discusión regional sobre esas regulaciones para tener un marco real que funcione en América Latina y el Caribe, que ayude a los diferentes países a trabajar en regulaciones nacionales que sigan los marcos internacionales/regionales.

2.7. Marco institucional y capacidades regulatorias

Para desarrollar nueva regulación sobre IA, protección de datos y sanción de delitos cibernéticos, debemos considerar diferentes aspectos, la prioridad que los gobiernos otorgan a estos temas, la disponibilidad de infraestructura, el conocimiento y la capacitación de los funcionarios públicos, así como policías y jueces. Es necesario analizar las acciones de los países de la región para detectar buenas prácticas y obstáculos que impidan la implementación de nuevos procesos, analizando que las capacidades institucionales varían considerablemente en la región.

Por ejemplo, la ANPD (Agencia nacional de protección de datos) de Brasil publicó un Estudio Preliminar sobre IA Generativa en noviembre de 2024, que examina cómo la legislación vigente en materia de protección de datos (LGPD) puede aplicarse a los sistemas de IA generativa y subraya la necesidad de transparencia, necesidad y orientación técnica para los actores públicos y privados [17]. Asimismo, el proyecto de ley de IA en Brasil (Proyecto de Ley n.º 2.338/2023) asigna funciones de supervisión a la ANPD, con el objetivo de coordinar la regulación de los sistemas de IA bajo una clasificación basada en riesgos [18].

En Uruguay, el Índice Latinoamericano de IA (ILIA 2024) reconoce las fortalezas del país en cuanto a capacidades de datos y excelencia en gobernanza, incluyendo la inversión en investigación, innovación y desarrollo de código abierto. Sin embargo, también señala la falta de talento, especialmente en educación y formación profesional en IA [19].

---

[15] Codigo Penal Bolivia Libro Primero Parte General Título I La Ley Penal Capítulo Único Reglas Para Su Aplicación. (N.D.). Https://Www.Oas.Org/Juridico/Spanish/Gapeca_Sp_Docs_Bol1.Pdf

[16] Observatorio de Ciberseguridad en América Latina y el Caribe. (2025). América Latina y el Caribe: Escalando la Escalera de la Ciberseguridad. GFCE. https://www.thegfce.org/news/latin-america-and-the-caribbean-climbing-the-cybersecurity-ladder/

[17]ANPD (Autoridad Nacional de Protección de Dados). (2024, 29 de noviembre). Estudio preliminar sobre IA generativa. https://www.fpf.org/blog/brazils-anpd-preliminary-study-on-generative-ai-highlights-the-dual-nature-of-data-protection-law-balancing-rights-with-technological-innovation/

[18]White & Case. (6 de junio de 2025). AI Watch: Seguimiento regulatorio global – Brasil. https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-brazil

[19]Consejo Nacional de Inteligencia Artificial (CENIA). (2024). ILIA 2024: Inteligencia Artificial Latinoamericana Índice . CEPAL. https://www.cepal.org/es/notas/ilia-2024-evaluando-la-preparacion-y-el-progreso-de-la-ia-en-america-latina

De igual manera, países como México, Argentina, Colombia, etc., cuentan con autoridades de protección de datos y estrategias de ciberseguridad, pero enfrentan limitaciones de recursos, una coordinación interinstitucional deficiente y a menudo, carecen de personal especializado o infraestructura para aplicar las leyes eficazmente. Estos problemas ralentizan la implementación de las regulaciones más allá de su promulgación formal.

2.9 **Grado de anticipación y resiliencia regulatoria y participación y representación de múltiples partes interesadas**

La mayoría de las leyes de la región son reactivas y no consideran la rápida evolución de la IA ni la ciberdelincuencia. Brasil es una excepción parcial con su proyecto de ley de IA basado en riesgos, que busca prever nuevos desafíos regulatorios. Otros países, como Chile y República Dominicana, están desarrollando agendas de ciberseguridad o digitales para actualizar sus regulaciones internas y adaptar las leyes existentes a las tecnologías emergentes.

En Bolivia, durante los primeros seis meses del año, se presentaron dos proyectos de ley para la regulación de la IA, a pesar de que aún no existe una regulación integral de la protección de datos y ciberseguridad. Por lo tanto, resulta ilustrativo lo que están haciendo otros países de la región, sería más adecuado seguir las recomendaciones de organismos regionales como la Organización de los Estados Americanos (OEA), que abogan no solo por una regulación específica de la IA, sino también por marcos más amplios de ciberseguridad y regulación digital que consideren los cambios tecnológicos, los plazos de implementación y los riesgos en constante evolución.

La resiliencia regulatoria requiere cláusulas de revisión periódica, evaluaciones de impacto y mecanismos como entornos de prueba regulatorios para probar tecnologías. Como argumentan algunos analistas políticos, regular la IA en una fase exponencial significa predecir "dónde estará la puerta cuando te subas al tren", es decir, diseñar leyes que anticipen el cambio en lugar de simplemente reaccionar a él.

El diseño de políticas debe incluir al gobierno, el sector privado, la academia, la sociedad civil y los grupos históricamente excluidos. Por ejemplo, el mapeo regulatorio de Access Now en América Latina [20]destaca la importancia de la consulta multisectorial con actores de la sociedad civil y de derechos humanos para la legitimidad y la inclusión. La baja participación de las mujeres en la I+D de IA sigue siendo un problema, ILIA 2024 informa que, incluso en los países líderes, lograr una participación equitativa de género en la investigación y el desarrollo de IA sigue siendo un desafío [21].

3. Metodología

3.1 Desafíos comunes: obsolescencia, fragmentación y falta de interoperabilidad

La realización del trabajo empírico implicó desafíos logísticos y sustantivos. El primero fue la programación: coordinar entrevistas con profesionales de siete países resultó complejo debido a las agendas de los profesionales, calendarios institucionales y obligaciones profesionales. Para superar esto, la investigación se basó en una planificación flexible y plataformas virtuales como principal vía de interacción. En total, se realizaron trece entrevistas virtuales y una presencial con un participante del programa Líderes de LACNIC en Argentina. La entrevista presencial

[20]Acceso ahora. (2024). Mapeo regulatorio sobre inteligencia artificial en América Latina. https://www.accessnow.org/publication/regulatory-mapping-on-artificial-intelligence-in-latin-america/

[21]Índice Latinoamericano de Inteligencia Artificial (ILIA). (2024). ILIA 2024: Evaluación de la preparación y el progreso de la IA en América Latina. CEPAL/CENIA. https://www.cepal.org/en/notes/ilia-2024-evaluating-ai-readiness-and-progress-latin-america

resultó significativamente más cercana entre la investigadora y la entrevistada, permitiendo una observación más detallada de las señales no verbales y creando un ambiente más fluido y abierto.

El segundo desafío se relacionó con el equilibrio entre confidencialidad y transparencia. Desde el inicio, el proyecto buscó minimizar el anonimato para fortalecer la credibilidad y trazabilidad de los hallazgos. A todos los entrevistados se les solicitó el consentimiento explícito para publicar sus nombres y roles profesionales. Trece estuvieron de acuerdo, mientras que uno solicitó el anonimato, lo cual llevó a una entrevista adicional buscando que los 14 entrevistados y entrevistadas tengan los perfiles públicos para fines de la investigación. Este resultado es inusual en estudios de gobernanza regional y refleja la confianza generada durante el proceso. También revela una compensación metodológica, el anonimato fomenta la franqueza, pero reduce la citabilidad, mientras que la atribución proporciona transparencia pero puede limitar la divulgación. Lograr una apertura casi total en todas las jurisdicciones fue, por lo tanto, el desafío de trabajo de campo más exigente, pero también enriqueció el estudio con perspectivas atribuibles que mejoran su valor explicativo.

3.1. Justificación del enfoque cualitativo

Se optó por un enfoque cualitativo porque el estudio busca no solo analizar textos normativos y documentos de política, sino también comprender cómo estos marcos operan en la práctica y cómo los perciben los profesionales responsables de su diseño e implementación. El análisis documental por sí solo no puede captar las dinámicas sociopolíticas, las capacidades institucionales ni las desigualdades estructurales que configuran la gobernanza en América Latina y el Caribe.

Por lo tanto, se seleccionaron las entrevistas semiestructuradas como instrumento principal, ya que combinan comparabilidad y flexibilidad. Una entrevista estructurada habría limitado el análisis, ignorando importantes diferencias nacionales. Por ejemplo, en Bolivia habría sido inapropiado preguntar sobre la conformidad con el RGPD dada la ausencia de una ley de protección de datos, mientras que en Brasil o Chile estas preguntas fueron fundamentales. Las entrevistas semiestructuradas permitieron al investigador adaptarse a estas variaciones contextuales, garantizando al mismo tiempo un marco de análisis coherente.

Este diseño también se alinea con el objetivo general del proyecto, combinar el análisis documental con la evidencia de campo, integrando textos legales con experiencias profesionales y conocimiento del entorno. Al captar cómo los actores clave interpretan las lagunas y posibilidades regulatorias, el enfoque cualitativo revela dimensiones de la gobernanza adaptativa que no pueden deducirse únicamente de los estatutos.

3.2. Selección de participantes para las entrevistas

Los participantes se identificaron mediante un muestreo intencional, priorizando a personas con reconocida experiencia y trayectoria en los campos del derecho digital, la gobernanza de la IA, la protección de datos o la ciberdelincuencia. Uno de los principales recursos fue el registro de abogados afiliados a la Federación. Iberoamericana de Asociaciones de Derecho e Informática (FIADI), que proporcionó un grupo confiable de profesionales con credenciales reconocidas. Se identificaron candidatos adicionales mediante publicaciones académicas, participación en eventos regionales (como ISOC, Internet Society) y redes profesionales.

En total, se entrevistó a catorce participantes, dos de cada uno de los siete países analizados (Argentina, Bolivia, Brasil, Chile, Colombia, República Dominicana y México). Esta distribución garantizó el equilibrio geográfico y la diversidad sectorial. La muestra incluyó a

responsables políticos, académicos, miembros de agencias de protección de datos y ciberseguridad, defensores de los derechos digitales, líderes del sector privado y sociedad civil.

3.3. Consentimiento, anonimato

Todos los participantes fueron informados con antelación sobre los objetivos de la investigación, el uso previsto de sus testimonios y su derecho a la confidencialidad. Catorce de los participantes autorizaron explícitamente la publicación de sus nombres y funciones profesionales, mientras que uno solicitó el anonimato, por lo cual no se añadió su entrevista dentro del análisis final.

Esta distribución tiene importantes implicaciones metodológicas. El predominio de testimonios no anónimos mejora la transparencia, fortalece la credibilidad del análisis y permite a los lectores vincular los argumentos con las funciones institucionales. Al mismo tiempo, el único caso de anonimato ilustra el valor de la confidencialidad en contextos donde pueden existir riesgos profesionales o políticos.

3.4. Formatos de entrevistas y reflexividad del investigador

Las entrevistas semiestructuradas fueron guiadas por un protocolo dividido en cuatro secciones temáticas:

- Desarrollo de los derechos digitales y los derechos humanos en la gobernanza de la tecnología,
- Desarrollo de políticas de protección de datos y prácticas institucionales,
- Desarrollo de políticas de ciberseguridad y ciberdelincuencia,
- Desarrollo de políticas de inteligencia artificial.

Cada entrevista incluyó un componente transversal para la identificación de brechas, obstáculos y puntos de mejora en los marcos de gobernanza nacional y regional, así como una evaluación de la participación e inclusión multisectoriales. Esto permitió no solo evaluar la existencia formal de leyes o estrategias, sino también comprender su funcionamiento en la práctica, los desafíos que enfrentan y las reformas que podrían fortalecer su eficacia.

En la práctica, se realizaron trece entrevistas virtuales y una presencial con un participante del programa Líderes de LACNIC. El formato presencial resultó especialmente valioso, generando una conversación más abierta y participativa, mientras que las entrevistas virtuales (con cámaras encendidas cuando fue posible) permitieron observar los gestos y el tono, aproximándose a la dinámica presencial.

Algunas respuestas confirmaron las expectativas (como el escepticismo sobre la implantación de los modelos europeos), mientras que otras fueron inesperadas (como la idea de pensar en mayor capacitación en habilidades digitales, antes que en normativa nacionales). El registro de las perspectivas, tanto anticipadas como imprevistas, reforzó la transparencia y la solidez de los hallazgos.

4. Análisis/Mapeo de buenas prácticas y modelos flexibles/ Entrevistas con profesionales regionales

4.1. Experiencias internacionales y regionales de gobernanza adaptativa

A nivel mundial, la Unión Europea está avanzando con la Ley de IA, que establece un enfoque basado en el riesgo que prohíbe los sistemas inaceptables y exige evaluaciones de impacto para

aplicaciones de alto riesgo. Canadá ha implementado la Evaluación de Impacto Algorítmico (AIA), que exige a los organismos públicos evaluar los riesgos antes de implementar sistemas automatizados de toma de decisiones. El Reino Unido ha sido pionero en entornos de pruebas regulatorios, que permiten a las empresas probar aplicaciones innovadoras de IA en condiciones controladas y con supervisión regulatoria.

En términos de inclusión y equidad, el Índice Global de IA Responsable (GIRAI) destaca que solo 24 países a nivel mundial abordan la igualdad de género en sus marcos de IA, lo que revela una brecha global significativa en la integración de las perspectivas de derechos humanos en la gobernanza tecnológica[22]. Estos ejemplos muestran que la gobernanza adaptativa a menudo combina el derecho vinculante (regulaciones y códigos vinculantes) con el derecho indicativo (directrices éticas, códigos de conducta, declaraciones de principios) y mecanismos experimentales como los entornos de pruebas, combinando la certidumbre regulatoria con la flexibilidad para la innovación.

En América Latina y el Caribe, algunos países han comenzado a explorar enfoques similares. Uruguay ha promovido agendas digitales participativas que incorporan aportaciones multisectoriales, en particular del ámbito académico y la sociedad civil. México elaboró un borrador de Estrategia Nacional de IA con énfasis explícito en la inclusividad, así como la creación de normas creadas en ciertos estados. Brasil abrió audiencias públicas durante el debate de su proyecto de ley de IA, un mecanismo de consulta importante, aunque imperfecto, dada la gran participación del sector privado.

Según las entrevistas realizadas para este estudio, profesionales de toda la región coincidieron en que “replicar la Ley de IA de la UE sin adaptación, trae conflictos y problemas de implementación a nivel institucional, político y social”. Haciendo hincapié en que una gobernanza eficaz requiere enfoques regionalizados y específicos para cada contexto, en lugar de la importación generalizada de modelos extranjeros.

Además, muchos países de América Latina y el Caribe carecen de la capacidad institucional, los recursos financieros y la experiencia técnica para desarrollar estrategias comparables a las de la Unión Europea, Canadá o el Reino Unido. Esta asimetría limita su capacidad para implementar evaluaciones de impacto algorítmicas, mantener entornos de pruebas regulatorios o establecer organismos especializados de supervisión de la IA (West, 2024) [23]. Esto pone de relieve la importancia de contar con modelos de gobernanza adaptativos y colaborativos que puedan operar eficazmente en entornos con recursos limitados, garantizando que la innovación tecnológica no profundice las desigualdades estructurales.

4.2 Casos exitosos de co-creación y regulación basada en principios

Uruguay ejemplifica buenas prácticas mediante la co-creación de su Agenda Digital 2025 [24], donde acuerdos multisectoriales garantizaron la inclusión de diversas perspectivas y la protección de los derechos fundamentales. Chile lanzó consultas públicas sobre su política de datos, invitando a una amplia participación del mundo académico, la sociedad civil y la industria. De igual manera, la "Radiografía Regulatoria" de Access Now demuestra cómo los

---

[22]Gobierno de Canadá y Agencia de los Estados Unidos para el Desarrollo Internacional (2024). Índice Global de IA Responsable: Edición Corregida. Agata Data. https://agatadata.com/wp-content/uploads/2024/11/Global-Index-on-Responsible-AI-2024-Corrected-Edition-25_10_24-Gobierno-de-Canada-y-USAID.pdf

[23]West, DM (2024). Regulación inteligente de la IA: Estrategias para los responsables de políticas públicas en América Latina. Brookings Institution. https://www.brookings.edu/articles/smart-ai-regulation-strategies-for-latin-american-policymakers

[24]Uruguay Digital. (2021). Agenda Uruguay Digital 2025. Gobierno de Uruguay. https://dig.watch/resource/agenda-uruguay-digital-2025

procesos de diagnóstico colaborativo pueden fortalecer la transparencia y la inclusión al incorporar experiencia externa en el diseño de políticas.

Estas experiencias co-creadas reflejan una preferencia por la regulación basada en principios en lugar de normas prescriptivas rígidas. Al incorporar principios como la protección de derechos, la transparencia, la rendición de cuentas y la no discriminación, estos marcos conservan la flexibilidad necesaria para evolucionar junto con los avances tecnológicos.

Las personas entrevistadas en toda la región destacaron la importancia de incluir explícitamente en estos procesos a las mujeres, los pueblos indígenas, las comunidades afrodescendientes y otros grupos históricamente marginados. Su inclusión no solo refuerza la legitimidad, sino que también contribuye a la justicia distributiva al garantizar que los marcos de gobernanza aborden las diversas realidades sociales en lugar de reforzar las desigualdades existentes.

4.3 Mecanismos de gobernanza distribuida y regulación en evolución

La gobernanza distribuida se refiere a la distribución del poder de decisión entre gobiernos, reguladores, sociedad civil, academia y sector privado. Este modelo se aleja de la regulación centrada en el Estado y promueve el diseño y la supervisión colaborativos. En América Latina y el Caribe, plataformas como el Foro Latinoamericano y del Caribe de Gobernanza de Internet (LACIGF) y las iniciativas de LACNIC han sido fundamentales para crear espacios de diálogo horizontal, desarrollar conjuntamente estándares técnicos y de políticas comunes.

Organizaciones internacionales y centros de estudios proponen nuevas innovaciones institucionales. Por ejemplo, Brookings[25] recomienda establecer institutos nacionales o regionales de seguridad de la IA, armonizar los estándares de datos compartidos y desarrollar entornos de pruebas regulatorios para la experimentación con IA en sandboxes regulatorios antes de su implementación a gran escala. Mecanismos como los contratos inteligentes regulados y las infraestructuras de datos compartidos ilustran aún más cómo la gobernanza puede evolucionar junto con las tecnologías emergentes.

La evidencia de las entrevistas confirma que los profesionales regionales perciben la gobernanza distribuida como necesaria y desafiante. Por un lado, permite una participación más amplia, la actualización continua y la cooperación transfronteriza. Por otro lado, exige la coordinación entre actores con niveles muy diferentes de capacidad institucional y recursos. Los participantes enfatizaron repetidamente que la cooperación regional es crucial para evitar la fragmentación de las regulaciones nacionales y fortalecer la resiliencia colectiva frente a riesgos transnacionales como la ciberdelincuencia, los sesgos algorítmicos y la monopolización digital.

En definitiva, estas prácticas ilustran que la regulación adaptativa en América Latina y el Caribe requiere no solo marcos jurídicos formales, sino también ecosistemas institucionales sólidos capaces de actualizar las normas, coordinar a los actores interesados e integrar la participación ciudadana. Si bien aún incipientes, las experiencias de la región apuntan a la viabilidad de un modelo híbrido que combina derecho imperativo, regulación basada en principios, mecanismos experimentales y gobernanza distribuida para cerrar la brecha persistente entre la innovación tecnológica y la protección de los derechos.

---

[25] Levy Yeyati, E. (2025, May 22). Smart AI regulation strategies for Latin American policymakers. Brookings Institution. https://www.brookings.edu/articles/smart-ai-regulation-strategies-for-latin-american-policymakers/

Mapeo comparativo de la normativa sobre IA, protección de datos y ciberdelitos en Argentina, Bolivia, Brasil, Chile, Colombia, República Dominicana y México

Protección de datos

País	Regulación	Buenas prácticas	Áreas de mejora
Argentina	Ley 25.326 (2000) de Protección de Datos Personales, inspirada en la Directiva de la UE de 1995; complementada por la Ley 26.388 (2008) sobre delitos informáticos. Supervisada por la Agencia de Acceso a la Información Pública (AAIP).	Adopción temprana en América Latina de una ley integral de privacidad; reconocimiento del derecho de habeas data; papel activo de la AAIP en la emisión de directrices y la aplicación de sanciones.	Actualizar el marco para alinearlo con el RGPD y la Convención 108+; ampliar los poderes de ejecución de la AAIP; fortalecer las reglas para las transferencias transfronterizas; introducir obligaciones explícitas sobre privacidad por diseño, transparencia algorítmica y procesamiento de datos relacionado con IA.
Bolivia	No existe una ley específica de protección de datos; las normas en telecomunicaciones, banca y protección del consumidor están fragmentadas. Se discutieron algunos proyectos de ley, pero no se promulgaron.	Aplicación sectorial limitada (por ejemplo, la ASFI supervisa el uso de datos en los servicios financieros).	Promulgar una ley nacional de protección de datos armonizada con los estándares regionales; crear una autoridad independiente de protección de datos; garantizar derechos exigibles (acceso, borrado, portabilidad); regular los flujos transfronterizos; abordar los riesgos y la rendición de cuentas relacionados con la IA.
Brasil	Lei Geral de Proteção de Dados (LGPD, Ley 13.709/2018), vigente desde 2020; supervisado por la Autoridade Nacional de Proteção de Dados (ANPD). Complementado por leyes sectoriales (por ejemplo, Marco Civil da Internet 2014).	Marco inspirado en el RGPD; la ANPD supervisa activamente el cumplimiento, emite multas y promueve evaluaciones de impacto sobre la privacidad;	Ampliar la capacidad financiera e institucional de la ANPD; mejorar la aplicación de la ley a nivel subnacional; aclarar los mecanismos de transferencia transfronteriza; fortalecer la orientación sobre IA, datos biométricos y

		protección sólida de datos confidenciales y derechos de los interesados.	responsabilidad algorítmica.
Chile	Ley 19.628 (1999) sobre datos privados (obsoleta). En 2023, Chile aprobó una nueva Ley de Protección de Datos que crea una autoridad supervisora independiente, la cual entrará en vigor en 2026.	Reconocimiento constitucional de la privacidad y el habeas data; aplicación judicial de la proporcionalidad; aprobación de una ley moderna y alineada con los estándares internacionales .	Garantizar la implementación efectiva de la ley de 2026; garantizar la independencia y los recursos de la nueva autoridad; fortalecer los mecanismos de aplicación; emitir orientación específica sobre IA, elaboración de perfiles y decisiones automatizadas.
Colombia	Ley 1266 (2008) sobre datos financieros y Ley 1581 (2012) sobre protección de datos personales. Supervisada por la Superintendencia de Industria y Comercio (SIC).	Marco jurídico sólido; la SIC es un regulador activo, emite multas y proporciona orientación; la jurisprudencia del Tribunal Constitucional refuerza los derechos.	Actualizar el marco para abordar la IA y los datos biométricos; mejorar los mecanismos de adecuación; garantizar que los recursos del SIC coincidan con la carga de trabajo; mejorar la interoperabilidad regional.
República Dominicana	La Ley 172-13 (2013) regula los datos personales, basándose en la legislación española anterior al RGPD. Su supervisión está a cargo principalmente de la Superintendencia de Bancos.	Reconocimiento de los derechos de acceso y rectificación; intento pionero en el Caribe; cierta protección a los datos crediticios.	Modernizar el marco según los estándares GDPR/108+; ampliar el alcance más allá de los datos financieros; establecer una autoridad multisectorial independiente; regular las transferencias transfronterizas; agregar disposiciones para el uso de datos de IA.
México	Ley Federal de Protección de Datos Personales en Posesión de Particulares (2010) y Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (2017). Anteriormente supervisada por el INAI (desmantelada en 2023).	Reconocimiento de derechos ARCO (acceso, rectificación, cancelación, oposición); principio de rendición de cuentas; diferenciación entre régimen de	Restablecer la autoridad de supervisión independiente; armonizar los marcos federales y estatales; modernizar las reglas sobre inteligencia artificial, elaboración de perfiles y datos transfronterizos; fortalecer los mecanismos de quejas y recursos ciudadanos.

		datos públicos/privados.	

Inteligencia artificial

País	Regulación	Buenas prácticas	Áreas de mejora
Argentina	una ley integral de IA . La Disposición Ética 2/2023 establece principios vinculantes (supervisión humana, rendición de cuentas y equidad). La Resolución 161/2023 establece un programa nacional de transparencia y protección de datos. El Proyecto de Ley 3003-D-2024 propone un Marco de IA Responsable de amplio alcance.	Las directrices éticas enfatizan fuertemente la rendición de cuentas, la transparencia y la supervisión humana; el programa nacional aumenta la conciencia sobre los riesgos de la IA, la equidad y la rendición de cuentas democrática.	Promulgar rápidamente el proyecto de ley sobre IA responsable; integrar la gobernanza de la IA con la próxima reforma de protección de datos; fomentar un debate inclusivo entre múltiples partes interesadas y una participación intersectorial constante.
Bolivia	No existe una legislación específica sobre IA ni una estrategia nacional. Recientemente se han presentado dos proyectos de ley sobre IA en la Asamblea Legislativa sin una consulta exhaustiva.	----	Desarrollar una estrategia nacional integral sobre IA; adoptar directrices éticas sólidas; vincular la regulación de la IA con la legislación pendiente sobre protección de datos; crear capacidad institucional y técnica para una supervisión eficaz.
Brasil	La Estrategia Nacional de IA (2021) define los principios rectores (ética, transparencia, derechos humanos e innovación). El Proyecto de Ley de IA (PL 2338/2023) introduce una regulación basada en el riesgo, prohíbe la puntuación social y exige mecanismos estrictos de supervisión humana.	Consultas públicas amplias e inclusivas; uso innovador de entornos regulatorios seguros; orientación de la ANPD sobre rendición de cuentas algorítmica,	Aprobar e implementar el proyecto de ley de IA; reforzar la inclusión transparente de las partes interesadas; garantizar la coordinación con la LGPD, la legislación de ciberseguridad y políticas nacionales de innovación más amplias.

		equidad y PET; proyecto de ley alineado con los estándares internacionales de la OCDE y la UE.	
Chile	La Política Nacional de IA (2021) prioriza la ética, la innovación, los derechos humanos y la transparencia. Aún no existe una ley vinculante sobre IA, pero existen múltiples directrices y estrategias vigentes a nivel nacional.	Estrategia política plurianual; consultas nacionales abiertas; apoyo a la investigación y el desarrollo de IA y a iniciativas de desarrollo de talentos intersectoriales.	Convertir las directrices de política nacional en reglas vinculantes y exigibles; fortalecer la gobernanza integral de los datos; integrar la supervisión de la IA en la próxima Ley de Protección de Datos (en vigor desde 2026).
Colombia	La Política Nacional de Transformación Digital e IA (CONPES 3975, 2019) promueve el desarrollo responsable de la IA, la innovación pública y el crecimiento sostenible, aunque no es legalmente vinculante.	El manual de ética nacional fomenta la colaboración público-privada; proyectos piloto para probar la IA en múltiples sectores; orientación detallada sobre transparencia y rendición de cuentas algorítmica.	Redactar y aprobar una ley integral sobre IA; alinear la regulación con la próxima reforma de protección de datos; aumentar las inversiones en experiencia, investigación y mecanismos de evaluación de riesgos en IA.
República Dominicana	Actualmente no existe en el país ninguna regulación, legislación o estrategia nacional específica sobre IA.	-----	Crear un marco nacional inclusivo de IA; adoptar directrices éticas rigurosas; vincular la política de IA con los marcos de protección de datos y de ciberdelincuencia; fomentar la conciencia pública y la capacitación técnica.
México	La Estrategia Nacional de IA (2018) establece prioridades generales. Dos nuevas iniciativas legislativas sobre IA (2024) proponen sistemas de clasificación basados en riesgos y marcos regulatorios con alineamiento internacional.	Las propuestas legislativas incluyen categorías de riesgo escalonadas; la estrategia nacional fomenta la innovación en IA, la investigación científica y el	Aprobar una ley integral de IA; garantizar una consulta y un debate públicos inclusivos; alinear la regulación con los nuevos proyectos de ley de protección de datos y ciberseguridad; garantizar mecanismos sólidos de supervisión independiente.

		espíritu emprendedor en diferentes sectores.	

Ciberdelincuencia

País	Regulación	Buenas prácticas	Áreas de mejora
Argentina	La Ley 26.388 (2008) modifica el Código Penal para incluir los delitos digitales: acceso no autorizado, violación de las comunicaciones electrónicas y sabotaje de sistemas (15 días a 6 meses de prisión).	Inclusión temprana de los delitos informáticos en el código penal; definiciones claras de acceso no autorizado, sabotaje e intrusión digital.	Actualizar las sanciones por ransomware y ataques DDoS; mejorar los mecanismos de cooperación transfronteriza; aumentar la capacidad de respuesta rápida ante incidentes cibernéticos.
Bolivia	No existe una ley integral sobre delitos cibernéticos; disposiciones fragmentadas y obsoletas dispersas en múltiples códigos sin procedimientos especializados.	----	Promulgar una ley moderna que penalice la piratería informática, el ransomware y el robo de datos; crear unidades especializadas en delitos cibernéticos y un CSIRT nacional con la capacitación adecuada.
Brasil	Ley 12.737/2012 ("Ley Carolina Dieckmann ") tipifica como delito la invasión de dispositivos informáticos; penas de 3 meses a 1 año más multa; integrada al Marco Civil da Internet y a la LGPD.	Define delitos de invasión y factores agravantes (daño económico, funcionarios públicos); fuerte conexión con los marcos de protección de datos.	Modernizar la legislación para abordar el ransomware, las infracciones a gran escala y las amenazas impulsadas por IA; armonizarla con las regulaciones LGPD e IA; fortalecer las capacidades nacionales de ciberpolicía.
Chile	La Ley de Ciberseguridad 21.668 (aprobada en 2023, vigente en 2025) crea la	Establece una autoridad centralizada; obligaciones	Desarrollar una capacidad institucional más amplia y

	Agencia Nacional de Ciberseguridad (ANCI), exige el reporte de incidentes, obliga a los proveedores esenciales a aplicar estándares de seguridad y establece un Consejo Multisectorial.	específicas para cada sector; informes obligatorios; institucionaliza un modelo de gobernanza de la ciberseguridad de múltiples partes interesadas.	concienciar al público; alinear la nueva ley de ciberseguridad con la próxima reforma de protección de datos; ampliar la capacitación especializada en materia de ciberdelito y las campañas de prevención.
Colombia	La Ley 1273/2009 tipifica como delito el acceso no autorizado, la interceptación de datos, la obstrucción del sistema, el uso de malware, el phishing y el fraude, con penas de hasta 120 meses .	Alcance completo de los delitos; impacto disuasorio; define claramente diversas formas de ciberataques y fraude en línea .	Modernizar la legislación para abordar el ransomware y los delitos impulsados por IA; mejorar la cooperación con C4IR (Centro para la Cuarta División de Inteligencia) Revolución Industrial de Colombia) y marcos internacionales
República Dominicana	La Ley 53-07 sobre delitos y faltas de alta tecnología (2007) tipifica como delito los códigos de acceso ilegales, la clonación, la interceptación, el sabotaje y la alteración de datos.	Amplio alcance jurídico de los delitos reconocidos; legislación regional temprana; proporciona un marco jurídico disuasorio con efectos de ejecución reales.	Actualizar la ley para abordar las nuevas ciberamenazas relacionadas con la IA; crear una autoridad independiente contra los delitos cibernéticos; mejorar la coordinación con los marcos de protección de datos y las políticas de IA.
México	una ley integral contra la ciberdelincuencia. Disposiciones dispersas en leyes sectoriales. El Proyecto de Ley Nacional de Ciberseguridad (2023) propone un régimen sólido (derechos digitales, cooperación con el sector privado, agencia de ciberseguridad, fiscales especializados y base de datos de actores maliciosos).	Estrategia ENCS 2017; protocolo nacional de incidentes CERT-MX; proyecto de ley de 2023 describe un marco integral de ciberseguridad con una sólida visión institucional.	Aprobar el proyecto de ley sobre ciberseguridad; actualizar el código penal para cubrir los delitos de ransomware e IA; abordar las preocupaciones sobre extralimitación; coordinarse con las estrategias de protección de datos e IA.

4.4. Entrevistas y análisis participativo: análisis clave esperado

Se espera que las entrevistas revelen inquietudes compartidas en toda la región: el temor a que la inteligencia artificial pueda exacerbar las desigualdades existentes, el reconocimiento de la necesidad de adaptar los modelos regulatorios europeos a las realidades latinoamericanas y la conciencia de las debilidades institucionales, como recursos limitados, marcos fragmentados y escasa experiencia técnica. Los encuestados probablemente destacarán la ausencia de políticas sólidas de inclusión digital, la persistencia de la desigualdad de género en la investigación y el desarrollo de la IA, y la urgente necesidad de leyes armonizadas para abordar la ciberdelincuencia y otras amenazas tecnológicas. Al mismo tiempo, se anticipa un fuerte consenso sobre la importancia de fundamentar la gobernanza en los principios de derechos humanos y garantizar una participación multisectorial genuina (incluyendo a las comunidades históricamente excluidas) para construir enfoques regulatorios adaptativos, inclusivos y capaces de equilibrar la innovación con la protección de los derechos.

Perspectivas de las partes interesadas y mapeo de la preparación legal en materia de protección de datos, inteligencia artificial y regulación de los delitos cibernéticos: Resultados de entrevistas en siete países de América Latina y el Caribe

	Nombre y cargo	Derechos digitales	Protección de datos	Ciberdelincuencia	Buenas prácticas	Recomendaciones
BOLIVI	**Karina Medinaceli** Profesor de Derecho Informático de la Universidad Mayor de San Andrés. Tiene una maestría en Derecho e Informática y un doctorado en Sociedad de la Información. Ex consultor en telecomunicaciones y protección de datos, actual presidente de ISOC Bolivia y activo en redes regionales de ciberseguridad.	Bolivia carece de un marco coherente de derechos digitales (existen protecciones fragmentadas en el derecho civil, la jurisprudencia sobre habeas data, las regulaciones de telecomunicaciones y salud). Los tribunales han ido moldeando la privacidad y los derechos ARCO mediante litigios y jurisprudencia constitucional. Sin embargo, no existe una conciencia cultural: los ciudadanos, los funcionarios públicos y las instituciones a menudo hacen mal uso o exponen datos sensibles (por ejemplo, casos de VIH en hospitales públicos). La socialización, la educación digital y una amplia conciencia cívica son prioridades urgentes para construir un entorno que respete los derechos.	El proyecto de ley (2023) cumple con los estándares del RGPD, la OCDE, la APEC e Iberoamérica . Sin embargo, la escasa transparencia en su elaboración y la escasa retroalimentación institucional amenazan su legitimidad y su futura aplicación. El período legislativo , la capacitación profesional y la presencia de Oficiales de Protección de Datos son esenciales. La invisibilidad de Bolivia ante las grandes tecnológicas y la ausencia de una autoridad socavan las transferencias internacionales de datos, la cooperación regional y el cumplimiento de los estándares globales en constante evolución.	Las disposiciones vigentes (1997) son obsoletas y obsoletas. La falta de adopción del Convenio de Budapest, la falta de un sistema de procesamiento especializado y la debilidad de las unidades policiales obstaculizan gravemente la capacidad de aplicación de la ley. Las iniciativas existentes (proyectos de ley senatoriales, reapertura de unidades en 2018) carecieron de apoyo político y continuidad. Los ciclos de capacitación colapsan debido a las constantes rotaciones policiales, el desperdicio de recursos, la experiencia y el aprendizaje institucional a largo plazo. La continuidad institucional sigue siendo una debilidad estructural para la respuesta de Bolivia a la ciberdelincuencia.	La Agenda Digital 2025-2030 introduce la ciberseguridad como eje estratégico (liderada por AGTIC con la OEA y modelos regionales). El secreto sectorial (financiero, médico, telecomunicaciones) ofrece salvaguardias parciales. Alguna jurisprudencia ha aclarado las acciones de habeas data y privacidad. Bolivia también cuenta con experiencia académica y participación de la sociedad civil (Internet Bolivia, universidades, ISOC Bolivia), lo que genera una comunidad epistémica emergente con potencial para influir en el debate público y el diseño regulatorio futuro.	Priorizar una ley de PD alineada con la capacidad regulatoria y económica de Bolivia (autoridad por etapas, perfiles de OPD, vacancia) Legis). Impulsar una reforma coherente de la ciberdelincuencia (delitos modernos, adhesión a Budapest, policía especializada no rotatoria). Fortalecer la ciberseguridad con una estrategia nacional realista (basada en los modelos de la OEA/UIT, CERT sectoriales y notificación obligatoria de infracciones). Retrasar la regulación de la IA hasta que existan las bases de la PD y la ciberseguridad; en su lugar, promover propuestas académicas, profesionales y de múltiples partes interesadas para orientar eficazmente a los legisladores.
	Nombre y cargo	**Derechos digitales**	**Protección de datos**	**Ciberdelincuencia**	**Buenas prácticas**	**Recomendaciones**

BOLIVIA	**Ariel Agramont Loza** Presidente de la FIADI, Capítulo Boliviano Abogado e informático multidisciplinar, especializado en derecho TI, cibercrimen, legaltech, inteligencia artificial y gobernanza digital, con amplia experiencia académica y profesional.	El diseño de políticas debe ajustarse al modelo administrativo de Bolivia (los reguladores del sector ya supervisan la privacidad en la banca y las telecomunicaciones). El uso futuro de la IA debe basarse en bases legales explícitas y recursos constitucionales (distinguiendo entre privacidad y protección de datos). El capital humano existe, pero la financiación y la capacidad institucional limitan la protección efectiva de los derechos, especialmente contra las falsificaciones profundas y la clonación de voz que ponen en peligro la imagen, el honor y la reputación.	Se necesita una ley integral de protección de datos, alineada con la arquitectura regulatoria de Bolivia (ASFI, autoridad de telecomunicaciones) y complementada con procedimientos administrativos claros y amparo constitucional. Evitar la copia y pega de documentos (adaptar los principios de la UE a la aplicación local). Definir las funciones, la jurisdicción y los recursos en todas las agencias, garantizando la compatibilidad procesal con los litigios de privacidad y el cumplimiento normativo viable para los responsables y encargados del tratamiento.	Actualizar las disposiciones penales para reflejar los delitos modernos y las realidades probatorias (preservación digital, datos volátiles). Crear una fiscalía especializada y un poder judicial capacitado para gestionar los abusos facilitados por la IA y los casos transfronterizos. Adherirse al Convenio de Budapest (esto fortalecería la cooperación y armonizaría las investigaciones con los estándares internacionales), manteniendo al mismo tiempo las reformas dinámicas y actualizándolas periódicamente para seguir la evolución del modus operandi.	Aprovechar la supervisión sectorial existente (banca y telecomunicaciones) y los pilotos de IA en salud y justicia. Promover la coordinación interinstitucional, protocolos prácticos para la evidencia digital y capacitación específica para policías, fiscales y jueces. Fomentar la innovación privada (startups) mientras se planifica el uso estatal de la IA para reducir la burocracia y la corrupción (con evaluaciones de riesgos y controles auditables).	Promulgar una ley de prevención de delitos informáticos adaptada a las instituciones bolivianas (con procedimientos y recursos claros). Modernizar la ciberdelincuencia y unirse a Budapest. Establecer una fiscalía especializada en ciberdelincuencia y capacitación judicial. Regular la IA estatal mediante mandatos legales explícitos, evaluaciones de impacto de la protección de datos (EIPD) y entornos de pruebas graduales (biometría y justicia prioritarias). Priorizar una legislación perfeccionable y basada en expertos en lugar de un consenso máximo que frene los resultados (coordinación regional a través de la CAN y redes de expertos).
	Nombre y cargo	**Derechos digitales**	**Protección de datos**	**Ciberdelincuencia**	**Buenas prácticas**	**Recomendaciones**

	Félix Juan Rivera Aquino Abogado de TI, Especializado en derecho digital y tecnologías disruptivas, con un máster en LegalTech y un segundo máster en Protección de Datos. Experiencia en ciberseguridad, derecho de las telecomunicaciones, informática forense e IA en la justicia. Investigador activo de FIADI desde 2017, presenta anualmente sobre protección de datos y tecnologías emergentes.	El reconocimiento de los derechos digitales progresó con la Constitución de 2010, protegiendo explícitamente la privacidad de los datos. La Estrategia Nacional de IA (2023) enfatiza la gobernanza ética, los derechos de los ciudadanos y las salvaguardias contra las decisiones automatizadas. Sin embargo, las brechas institucionales dificultan su aplicación efectiva, ya que los ciudadanos a menudo carecen de mecanismos accesibles para reclamar sus derechos digitales fuera del sector bancario.	La Ley 172-13, inspirada en la ley derogada de España, presenta debilidades estructurales. La supervisión sigue limitada a los datos crediticios a cargo de la Superintendencia de Bancos. La ausencia de una autoridad independiente obliga a la judicialización, sobrecargando los tribunales. Las reformas legislativas en curso buscan una mayor supervisión, rendición de cuentas y salvaguardias contra las decisiones automatizadas, reflejando los principios del RGPD de proactividad y cumplimiento.	La ley de 2003-2004 sobre delitos de alta tecnología está obsoleta y carece de respuestas al phishing, el robo de identidad y las amenazas en constante evolución. El Centro Nacional de Ciberseguridad y la fiscalía especializada existen, pero siguen centralizados en la capital, lo que limita la cobertura nacional. El manejo de pruebas, como las capturas de pantalla, muestra fragilidad, lo que socava la credibilidad y la eficacia del procesamiento de los delitos cibernéticos.	El Centro Nacional de Ciberseguridad y la Estrategia Nacional de IA ofrecen un marco con visión de futuro que integra la ética, el desarrollo del talento y las colaboraciones público-privadas. La fiscalía especializada demuestra la atención institucional a la ciberdelincuencia. El reconocimiento constitucional de la protección de datos y los decretos presidenciales sobre ciberseguridad reflejan avances, aunque persisten deficiencias en la aplicación de la ley, los recursos y el alcance territorial.	Establecer una autoridad supervisora independiente para la protección de datos a fin de evitar la judicialización excesiva. Actualizar la legislación sobre ciberdelitos para abordar las nuevas amenazas digitales. Ampliar la formación de jueces, fiscales y policías en todo el país. Desarrollar un marco legislativo flexible con principios rectores generales. Implementar un código ético vinculante de IA para mitigar riesgos como los deepfakes.
	Nombre y cargo	**Derechos digitales**	**Protección de datos**	**Ciberdelincuencia**	**Buenas prácticas**	**Recomendaciones**

DOMINICAN	**Nicole María Suárez Uribe** Fundadora de NICTECH, firma de transformación digital que desarrolla soluciones responsables Soluciones tecnológicas. Abogado especializado en Derecho Administrativo y Gestión Pública Estratégica, con Magíster en Derecho Digital y Nuevas Tecnologías. Investigador en IA generativa para justicia, educación y gobernanza.	Los derechos digitales en República Dominicana siguen obsoletos, y las leyes no abordan los contextos en línea. La interpretación constitucional subsana lagunas, pero los grupos vulnerables siguen desprotegidos. La Agenda Digital Nacional 2030 y las políticas de innovación reconocen la inclusión digital, pero siguen siendo directrices no vinculantes. La brecha digital persiste, dejando a las poblaciones marginadas sin protecciones exigibles para sus derechos en línea.	La Ley 172-13 se centra estrictamente en los datos financieros, dejando sin cubrir otros sectores. Las autoridades electorales gestionan los datos biométricos de forma controvertida. Las peticiones de una Agencia Nacional de Protección de Datos ponen de relieve la urgente necesidad de reformas. Los proyectos de ley pendientes se ajustan a los estándares internacionales, pero aún no se han aprobado. Los ciudadanos dependen actualmente de instituciones fragmentadas como INDOTEL u OPTIC para obtener reparación.	La legislación sobre ciberdelincuencia está obsoleta e insuficiente ante las amenazas emergentes. El Centro Nacional de Ciberseguridad (C5I) coordina las respuestas, pero la confusión ciudadana sobre las instituciones socava su eficacia. Casos como las filtraciones de datos de pasaportes expuestas en la red oscura revelan graves vulnerabilidades. Las demoras judiciales debilitan la aplicación de la ley, dejando a las víctimas expuestas a pesar de la infraestructura técnica y los departamentos policiales especializados.	La Estrategia Nacional de Ciberseguridad 2030, la Agenda Digital y la hoja de ruta de IA reflejan avances en la alineación internacional, incluyendo el marco ético de IA de la UNESCO. El enfoque inclusivo en los grupos vulnerables demuestra conocimiento de las políticas. Las recientes propuestas legislativas sobre IA buscan una regulación más amplia e integral. Sin embargo, la dependencia de los modelos legales europeos corre el riesgo de implantaciones poco prácticas que ignoren las realidades locales.	Los legisladores deben priorizar la legislación inclusiva y participativa, involucrando al mundo académico, la sociedad civil y los grupos vulnerables. Evitar la regulación fragmentada y basada en modas (por ejemplo, leyes que solo se centran en deepfakes). Crear una Agencia de Protección de Datos independiente y modernizar los marcos de telecomunicaciones, ciberdelincuencia e inteligencia artificial. Priorizar la educación, la concienciación pública y las políticas contextuales para transformar los textos legales en protecciones prácticas que se ajusten a las necesidades locales.
	Nombre y cargo	**Derechos digitales**	**Protección de datos**	**Ciberdelincuencia**	**Buenas prácticas**	**Recomendaciones**

COLOMBIA	**Lucía Camacho** Pública Política Coordinadora Derechos Digitales Una ONG regional que trabaja en la intersección de los derechos humanos y la tecnología. Especializada en derechos digitales, gobernanza de datos y regulación de la IA, con amplia experiencia en el análisis de la legislación colombiana y latinoamericana. marcos, destacando tanto las oportunidades como desafíos institucionales.	La política digital colombiana es amplia, pero fragmentada. Carece de una arquitectura jurídica fundamental (gobernanza estatal de datos, acceso a la información, biometría, automatización). Los primeros trabajos sobre IA se basaron en ética no vinculante y entornos de pruebas; proyectos de ley recientes replican la taxonomía de riesgos de la UE sin trasplantar instituciones ni abordar los usos locales (biometría estatal, IA en los tribunales). El debate está activo; aún no se ha promulgado ninguna ley de IA.	Ley de DP de 2012; la autoridad (SIC/ Delegación de DP) depende del Ejecutivo, sin independencia orgánica ni financiera. Emite directrices (PIA, cumplimiento normativo), pero carece de decisiones clave sobre procesamiento automatizado/IA. El alcance territorial es limitado: las grandes tecnológicas impugnan la jurisdicción cuando no tienen su domicilio en Colombia. Las restricciones fiscales reducen la capacidad, lo que debilita estructuralmente la aplicación de la ley y la supervisión transfronteriza.	Colombia se adhirió a la Convención de Budapest y penalizó delitos clásicos (acceso no autorizado, robo de datos, suplantación de identidad). A nivel regional, las leyes de ciberdelito pueden utilizarse indebidamente para reprimir la libertad de expresión (p. ej., leyes sobre noticias falsas). Los daños emergentes (identidad facilitada por deepfakes/violencia sexual) siguen sin abordarse adecuadamente; las referencias comparativas señalan nuevos delitos relacionados con la IA en el extranjero. Las actualizaciones legislativas deben evitar una deriva restrictiva de la libertad de expresión y, al mismo tiempo, abordar los nuevos delitos facilitados por la IA.	Las capacidades de seguridad y ciberseguridad han evolucionado más allá de una perspectiva exclusivamente defensiva hacia la gestión de riesgos y las políticas estatales de seguridad digital. El sector judicial está desarrollando directrices sobre IA (influencia de la UNESCO). La capacidad sectorial varía considerablemente; la pandemia aceleró la adopción, pero la coherencia y la transparencia se retrasan. Reconocer la variabilidad sectorial es esencial para una gobernanza realista y aplicable.	Dejen de copiar y pegar el modelo de la UE. Construyan una arquitectura jurídica básica (gobernanza estatal de datos, normas biométricas, IA en la justicia), promulguen salvaguardias sectoriales y fortalezcan una Autoridad de Protección de Datos (APD) independiente, con recursos y alcance extraterritorial. Actualicen la ciberdelincuencia de forma específica para abarcar los daños provocados por la IA. Combatan la evasión jurisdiccional de las grandes tecnológicas mediante una aplicación coordinada y transnacional de la ley; garanticen la transparencia de las actividades de cabildeo y protejan el espacio cívico.
	Nombre y cargo	**Derechos digitales**	**Protección de datos**	**Ciberdelincuencia**	**Buenas prácticas**	**Recomendaciones**

COLOMBIA	**Julián Leguízamo** Abogado, graduado de la Universidad Santo Tomás, Filial Villavicencio, especializado en derecho penal y criminología. Trabajó en tribunales municipales y de circuito, incluidos tribunales especializados en crimen organizado y lavado de dinero.	Colombia reconoce garantías constitucionales como el habeas data, la privacidad y la libertad de expresión; sin embargo, su implementación efectiva sigue siendo inconsistente. Leguízamo subraya que la moderación algorítmica y la censura impulsada por las plataformas socavan cada vez más estos derechos, generando asimetrías de poder entre los usuarios y las corporaciones digitales. Sin una interpretación judicial proactiva y la conciencia de los impactos tecnológicos, los derechos digitales corren el riesgo de quedar en mera declaración en lugar de ser exigibles en la práctica.	Colombia aplica un modelo híbrido mediante la Ley 1581/2012, que combina protecciones generales con regulaciones sectoriales en ámbitos como la banca y las telecomunicaciones. Esta estructura refleja adaptabilidad, pero adolece de una supervisión deficiente y una capacidad institucional limitada. Para Leguízamo , la protección de datos requiere autoridades supervisoras independientes con facultades sancionadoras, evaluaciones sistemáticas del impacto en la privacidad y mecanismos institucionales más sólidos para transformar las garantías formales en protecciones tangibles para los usuarios.	Identifica graves deficiencias en la legislación colombiana sobre ciberdelitos, que sigue anclada en marcos anticuados y una redacción legal imprecisa. Esta vaguedad socava la seguridad jurídica y obstaculiza la persecución judicial efectiva. Amenazas emergentes como el ransomware, el cibersabotaje y la ciberguerra exigen una modernización legislativa, junto con fiscales, jueces y unidades de investigación especializados. Sin estas reformas, Colombia corre el riesgo de una vulnerabilidad sistémica ante ciberataques transnacionales.	A pesar de las debilidades estructurales, Leguízamo reconoce avances en el sector financiero, donde los estándares de cumplimiento y los protocolos de ciberseguridad superan los promedios regionales, y en la labor de la Agencia Nacional de Seguridad Digital. Destaca que la capacitación judicial sostenida, la integración de la alfabetización digital en la práctica jurídica y la institucionalización de la experiencia técnica son indispensables para integrar la protección de los derechos en la gobernanza y la aplicación de la ley.	Recomienda. Propone reformar los delitos existentes mediante la introducción de circunstancias agravantes específicas para el ámbito digital (como el robo cibernético o la difamación), en lugar de proliferar nuevas y fragmentadas categorías penales. Las reformas legislativas deben ser flexibles, revisarse periódicamente y adaptarse al contexto, evitando la adopción acrítica de modelos extranjeros. Para Colombia, el progreso genuino depende de una regulación pragmática y adaptada a las necesidades locales que priorice la coordinación institucional, la exigibilidad y la resiliencia ante las amenazas tecnológicas en constante evolución.
	Nombre y cargo	**Derechos digitales**	**Protección de datos**	**Ciberdelincuencia**	**Buenas prácticas**	**Recomendaciones**

CHILE	**Patricia Reyes** Vicedecana de Derecho, Universidad de Valparaíso Abogada y profesora con más de 30 años de experiencia en derecho y tecnología. Desarrolló sistemas de información jurídica para el Congreso chileno, dirige la cátedra de Derecho y Tecnología en la Universidad de Valparaíso desde 2010 y participa en FIADI, el Instituto Chileno de Derecho y Tecnología, y en comités de expertos sobre gobernanza digital.	Chile modernizó su marco de referencia en materia de derechos digitales: una Ley de Transformación Digital garantiza la identidad digital, la interoperabilidad y la calidad de los datos; la Constitución reconoce los "neuroderechos" que protegen la integridad mental. Sin embargo, la proliferación de agencias corre el riesgo de fragmentar la gobernanza, y los organismos públicos implementan IA sin una base legal explícita (especialmente en los ámbitos de la justicia y la seguridad pública), lo que genera opacidad e incertidumbre jurídica que socava los derechos.	La ley de privacidad de 1999 permitió el marketing masivo y unas garantías deficientes. Una nueva Ley de Protección de Datos (aprobada en 2024; en vigor en 2025) se ajusta a los estándares de la UE y crea una Autoridad de Protección de Datos (APD) especializada. Principales desafíos: baja cultura de cumplimiento social, necesidad de nombramientos técnicos (no políticos) y una sólida coordinación interinstitucional (APD, Consejo de Transparencia, Secretaría Digital del Gobierno).	Chile promulgó una histórica Ley Marco de Ciberseguridad (2025), que incluye una Agencia Nacional de Ciberseguridad, coordinación de respuesta a incidentes, organismos de acreditación y un régimen de "operadores de vital importancia" que exige evaluaciones de riesgos, planes de seguridad, certificación, informes y la designación de oficiales de ciberseguridad, con importantes sanciones. Su implementación está en marcha en contextos civiles, de infraestructura crítica y de defensa.	Una sólida voluntad política permitió mejoras rápidas: marco de ciberseguridad, Ley de Transformación Digital, Política Nacional de IA actualizada (alineada con la UNESCO y la UE, basada en riesgos) y un activo proceso de normalización por parte de organismos sectoriales. Las obligaciones de cumplimiento normativo (gestión de riesgos, presentación de informes, certificación) reflejan modelos avanzados y se están implementando mediante directrices, comités interministeriales y normas sectoriales, incluyendo las de defensa y servicios críticos.	Prevenir la fragmentación regulatoria: exigir una orientación coordinada y jerárquica entre las agencias. Garantizar la independencia y el liderazgo técnico de la DPA. Exigir autorización legal explícita y entornos de pruebas con evaluación de impacto antes de implementar IA de alto riesgo (biometría, vigilancia, apoyo a la toma de decisiones judiciales). Priorizar la concienciación a nivel nacional y el cambio de prácticas para los controladores y la ciudadanía. Continuar perfeccionando el proyecto de ley de IA con salvaguardas de los derechos fundamentales y normas adaptables y actualizables.
	Nombre y cargo	**Derechos digitales**	**Protección de datos**	**Ciberdelincuencia**	**Buenas prácticas**	**Recomendaciones**

CHILE	**Basilio Belmar Rivas** Abogado, Magíster en Derecho Público, actualmente Director Jurídico de Fundación Ronda y Profesor Asistente de la Universidad de Valparaíso. Se especializa en derecho digital desde 2016, co-impartiendo el seminario “Derecho y Tecnología” y talleres sobre redacción legislativa.	Chile está experimentando una transformación significativa en materia de derechos digitales, con la entrada en vigor de una Ley de Protección de Datos reformada a finales de 2025. Esta ley incluye derechos ARCO más amplios, nuevas obligaciones para los responsables del tratamiento y la creación de una Agencia de Protección de Datos. Si bien se inspiran en el RGPD y otros modelos globales, los legisladores chilenos adaptaron las disposiciones a las realidades nacionales. Persisten los desafíos en la concienciación pública, las prácticas culturales y la conciliación de la protección de datos con el acceso a la información pública.	La ley reformada establece una Agencia de Protección de Datos independiente, Delegados de Protección de Datos (OPD), sanciones más estrictas y normas detalladas para las transferencias internacionales. Chile aspira a la adecuación a las normas de la UE, considerando también los estándares japoneses y coreanos. Su implementación requiere nuevas regulaciones, normas técnicas y mayores presupuestos. Si bien Chile ha avanzado considerablemente, se necesita una educación generalizada para garantizar que los ciudadanos y las organizaciones comprendan plenamente las obligaciones de cumplimiento normativo y la importancia de la gestión de datos personales.	Las reformas recientes modernizaron la legislación obsoleta de la década de 1990, alineándose con la Convención de Budapest. Se promulgó una Ley Nacional de Ciberseguridad y se está creando un organismo para coordinar las políticas de seguridad. Las brigadas policiales contra el cibercrimen existen principalmente en las grandes ciudades (Santiago, Valparaíso, Concepción), lo que limita la capacidad de respuesta de las regiones más pequeñas. Si bien la legislación es sólida, su implementación efectiva enfrenta desafíos presupuestarios e institucionales, y los organismos de investigación requieren mayor especialización técnica para afrontar las amenazas en constante evolución.	Chile demuestra buenas prácticas mediante la colaboración entre múltiples actores, la transformación digital de los servicios públicos y la integración de sistemas de identificación digital. Las instituciones públicas colaboran con universidades y la sociedad civil en eventos como "Mis Datos y Yo ", promoviendo la concientización y el diálogo sobre políticas. La nueva estrategia de gobierno digital y la digitalización obligatoria de los procesos estatales para 2027 son impulsores clave del cambio estructural, posicionando a Chile como un referente regional en modernización institucional.	Chile debería fortalecer la capacidad técnica en materia de aplicación de la ley, ampliar las unidades regionales de ciberdelincuencia y garantizar la financiación adecuada para la nueva Agencia de Protección de Datos. La educación y la concienciación siguen siendo urgentes para cambiar las prácticas culturales en relación con la divulgación indiscriminada de datos. A nivel regional, el progreso de Chile podría inspirar marcos armonizados, pero la sostenibilidad depende de la adaptación de los modelos externos a las realidades locales, garantizando que las leyes sigan siendo prácticas, aplicables y acordes con los valores democráticos y las necesidades sociales.
	Nombre y cargo	**Derechos digitales**	**Protección de datos**	**Ciberdelincuencia**	**Buenas prácticas**	**Recomendaciones**

ARGENTINA	**Bibiana Luz Clara** Presidenta de la Federación Iberoamericana de Asociaciones de Derecho e Informática (FIADI) Doctor en Derecho Procesal (Universidad de Salamanca), con Máster en Derecho de Internet (Campus Europeo). Profesor e investigador en la Universidad KS y profesor de posgrado en la UBA. Investigador, con comentarios. sobre la Ley de Firma Digital y trabaja en la mediación electrónica.	Los debates sobre políticas digitales siguen fragmentados, con marcos vinculantes limitados y contribuciones académicas notables que configuran el discurso. La polarización política ralentiza la aprobación de la legislación sobre IA y derechos digitales, dejando lagunas regulatorias. Los riesgos incluyen la pérdida de empleos, la erosión de los derechos laborales, las preocupaciones sobre los neuroderechos derivadas de las interfaces cerebro-computadora y la regulación del habla. Los dilemas éticos hacen hincapié en equilibrar la innovación con la protección efectiva de la dignidad humana.	La Ley 25.326 (2000) ha quedado obsoleta tras 25 años de cambios tecnológicos. Se necesita urgentemente una reforma para modernizar los derechos, la aplicación de la ley y los estándares de gobernanza de datos sensibles. El proyecto de ley de reforma anterior venció, por lo que requiere su reintroducción y consenso político. Las autoridades y los tribunales carecen de una sólida cultura de implementación, y aún dependen en gran medida del habeas data como medida de salvaguardia. La armonización con los modelos del RGPD es necesaria, pero debe reflejar las capacidades institucionales y las realidades de aplicación de la ley en Argentina.	Argentina modificó su Código Penal en 2008 para incluir los delitos informáticos y lo amplió con reformas graduales, como la captación de testigos (2013). Existen protocolos y herramientas de preservación de evidencia digital; sin embargo, la carga de trabajo, los retrasos y la escasez de recursos humanos retrasan los procedimientos, lo que conlleva el riesgo de pérdida de evidencia volátil. La ratificación por parte de Argentina del Convenio de Budapest fortalece la cooperación transfronteriza, pero siguen siendo cruciales en todo el país la actualización de protocolos y una respuesta judicial más rápida.	Argentina desarrolló sólidos protocolos de evidencia digital, instrumentos de orientación pública e iniciativas de capacitación sectorial. La reforma del Código Civil y Comercial (2015, vigente desde 2016) modernizó los contratos electrónicos, la protección al consumidor y las transacciones digitales. La Ley de Teletrabajo 27.555 (2021) estableció salvaguardas para el trabajo remoto. La Corte Suprema otorgó el mandato de gestión electrónica completa de casos, lo que mejoró la eficiencia y, al mismo tiempo, expuso lagunas procesales no resueltas que requieren una mayor consolidación legislativa y mecanismos de cumplimiento actualizados.	Actualizar con prontitud la Ley de Protección de Datos para alinearla con la adecuación del RGPD y las realidades de 2025. Mantener actualizaciones continuas en los marcos jurídicos penales, civiles y procesales. Ampliar la capacidad institucional para la investigación forense, la fiscalía y la judicatura. Establecer salvaguardas legales para los sistemas de IA de alto riesgo, como la biometría y la neurotecnología. Prepararse para los riesgos de la era cuántica con criptografía cuántica segura, formulación de políticas interdisciplinarias, mayor financiación y alfabetización digital continua para ciudadanos y profesionales.
	Nombre y cargo	**Derechos digitales**	**Protección de datos**	**Ciberdelincuencia**	**Buenas prácticas**	**Recomendaciones**

ARGENTINA	**María Trione** Abogado con estudios de posgrado en derecho tecnológico, derecho de la inteligencia artificial y gobernanza de internet. A través de Criando. En Digital, trabaja en consultoría, investigación y divulgación centrada en los derechos de la infancia y la protección de los menores en el entorno digital.	El marco de derechos digitales de Argentina está reconocido formalmente mediante el habeas data constitucional, pero su aplicación es deficiente e inconsistente. Las instituciones estatales con frecuencia manejan de forma indebida o exponen información sensible, y las reiteradas filtraciones a gran escala de bases de datos socavan la confianza pública. La ciudadanía rara vez exige rendición de cuentas, lo que refleja las brechas culturales en la concienciación, la educación y la socialización de los derechos digitales.	La Ley 25.326, aprobada en el año 2000, está obsoleta e insuficiente para las realidades tecnológicas actuales. Las propuestas de reforma inspiradas en el RGPD se estancaron en el Congreso, dejando a las instituciones sin garantías modernas ni mecanismos de cumplimiento adecuados. La autoridad de protección de datos carece de independencia, recursos y capacidad, lo que erosiona su legitimidad e impide una supervisión efectiva de los actores estatales y privados.	Argentina incorporó delitos cibernéticos como el acoso, la piratería informática y el fraude mediante sucesivas reformas penales. Si bien existen protocolos para la evidencia digital, los procesos judiciales siguen siendo lentos, las investigaciones carecen de fondos suficientes y los expertos especializados son escasos. Las demoras estructurales y las limitaciones de recursos dificultan la respuesta oportuna, lo que debilita la disuasión y frustra a las víctimas que requieren protección rápida en casos relacionados con la tecnología.	Argentina se ha adherido al Convenio de Budapest, lo que permite la cooperación transfronteriza en la persecución de los delitos cibernéticos. La jurisprudencia continúa perfeccionando las acciones de hábeas data y aclarando los estándares probatorios para entornos digitales. Universidades y grupos de investigación experimentan con marcos de gobernanza de la IA y debates éticos, lo que ofrece el potencial de definir futuras orientaciones políticas a pesar de las limitaciones institucionales.	Argentina debería actualizar urgentemente su ley de protección de datos para alinearla con los estándares internacionales, garantizando salvaguardias más sólidas, derechos conforme al RGPD y una autoridad reguladora autónoma. Es fundamental aumentar la financiación y la coordinación para la persecución de los delitos cibernéticos. Los programas de educación cívica deben concienciar a la ciudadanía sobre la privacidad y la rendición de cuentas. Finalmente, el despliegue de la IA, especialmente en contextos judiciales, requiere transparencia, directrices éticas y mecanismos de supervisión sólidos.
	Nombre y cargo	**Derechos digitales**	**Protección de datos**	**Ciberdelincuencia**	**Buenas prácticas**	**Recomendaciones**

BRAZIL	**Marina Meira** Abogada y Coordinadora de Políticas Públicas en Derechos Digitales . Ha trabajado extensamente en la sociedad civil brasileña en materia de protección del consumidor, derechos del niño y, en particular, protección de datos. Anteriormente, coordinó el programa nacional de Brasil contra la desinformación y colaboró en investigaciones internacionales. Su experiencia conecta la incidencia política, la regulación y los derechos digitales, con un enfoque regional en América Latina.	El marco brasileño para los derechos digitales se basa en el Marco Civil da Internet de 2014 y la LGPD de 2018. Ambos incorporan principios de derechos humanos como la neutralidad de la red, el debido proceso y la protección de datos sensibles. Si bien las normas son sólidas, su aplicación sigue siendo desigual. Los desafíos estructurales incluyen instituciones débiles, presupuestos insuficientes y una desconexión entre el reconocimiento legal y la conciencia ciudadana común sobre los derechos en entornos digitales.	La LGPD creó la Autoridad Nacional de Protección de Datos (ANPD), que goza de autonomía formal desde 2022, pero cuenta con recursos limitados. Si bien está en consonancia con los estándares internacionales, su aplicación práctica es deficiente. Se han aplicado pocas sanciones y la concienciación pública sigue siendo baja. La nueva legislación que restringe la elaboración de perfiles y la publicidad dirigida a menores supone un avance, pero las desigualdades estructurales y la fragilidad de las instituciones democráticas dificultan una protección de datos consistente.	Brasil carece de una ley unificada contra los delitos cibernéticos, basándose en disposiciones dispersas y a menudo obsoletas, como la ley de "pornografía vengativa" de 2012 y el estatuto de ciberacoso de 2021. La aplicación de la ley es inconsistente: las víctimas a menudo no denuncian los incidentes y las autoridades carecen de capacidad técnica y protocolos con perspectiva de género. Esto genera una percepción generalizada de impunidad, especialmente en lo que respecta a la violencia de género en línea y el manejo de pruebas digitales.	Brasil demuestra importantes buenas prácticas mediante la formulación de políticas con la participación de múltiples partes interesadas, donde el Tribunal Supremo Federal desempeña un papel de protección de derechos. La ANPD ha actuado contra abusos como la recopilación de datos biométricos de Worldcoin , mientras que las organizaciones de la sociedad civil monitorean los derechos digitales. Las nuevas leyes sobre protección infantil en plataformas digitales y la reciente Estrategia Nacional de Ciberseguridad (2025) destacan los avances. Las colaboraciones regionales de investigación, como los estudios sobre el comercio de datos personales en grupos de Telegram, fortalecen aún más la supervisión.	Brasil debería reforzar el presupuesto y el personal de la ANPD para fortalecer la aplicación de la ley, ampliar la educación pública sobre protección de datos y adoptar protocolos claros para la evidencia digital. Actualizar las leyes contra los delitos informáticos con una perspectiva de derechos humanos, garantizar salvaguardias contra el uso indebido de datos por parte del Estado y abordar las desigualdades estructurales, como el racismo, en los sistemas de IA son prioridades. La cooperación regional debería promover una gobernanza a medida en lugar de replicar directamente los modelos europeos.
	Nombre y cargo	**Derechos digitales**	**Protección de datos**	**Ciberdelincuencia**	**Buenas prácticas**	**Recomendaciones**

BRAZIL	**Dina Santana** Analista en Comercio Exterior, con Maestría en Administración Pública. Investigadora y candidata a doctorado en un Instituto Brasileño de Ciencia y Tecnología, vinculado al Ministerio de Ciencia y Tecnología. Miembro de ISOC, activa en espacios de LACNIC y miembro del grupo Mujeres en Ciberseguridad de la OEA. Con experiencia en políticas públicas, gobernanza digital y derechos del consumidor.	En Brasil, los derechos digitales han avanzado gracias a la Ley General de Protección de Datos (LGPD) de 2018 y su implementación en 2022, junto con la creación de la Autoridad Nacional de Protección de Datos (ANPD). Este marco institucional ha sido decisivo para promover la rendición de cuentas, la concienciación pública y mecanismos participativos como FALA.BR, que permiten a la ciudadanía participar directamente en los debates sobre políticas y los procesos de supervisión.	La LGPD representa un gran avance hacia la protección de datos, respaldada por las facultades regulatorias de la ANPD e iniciativas como los canales de denuncia y los experimentos de sandbox. Sin embargo, Brasil aún enfrenta desafíos para garantizar que la sociedad en general conozca la existencia de estos mecanismos. La divulgación y la educación públicas siguen siendo deficiencias clave para garantizar la aplicación efectiva de la ley y la participación ciudadana en la protección de los datos personales.	Brasil ha construido un sólido marco de ciberseguridad, reconocido mundialmente, ocupando el segundo lugar en el Índice Global de Ciberseguridad 2024 de la UIT. Instituciones como CGIBR, ANATEL, CEPRO y el Gabinete de Seguridad de la Presidencia se coordinan con los CSIRT de organismos públicos, universidades y empresas. A pesar de esta fortaleza institucional, la escasez de recursos humanos y la implementación desigual reducen la eficacia del sistema, especialmente en instituciones más pequeñas y regiones menos conectadas.	Entre las prácticas clave se incluyen la Política Nacional de Ciberseguridad (2023) y la Estrategia de Ciberseguridad Electrónica (2025), que proporcionan directrices estratégicas para la resiliencia. El país mantiene un modelo de gobernanza multisectorial con consultas públicas y organismos como el CGIBR que garantizan la participación. Si bien persisten los desafíos de interoperabilidad, Brasil demuestra una sólida capacidad institucional, lo que lo convierte en un referente regional, junto con Chile, en la estructuración de marcos integrales y participativos de ciberseguridad y gobernanza digital.	Dina enfatiza la urgencia de la alfabetización digital estructural y la concienciación ciudadana. Existen leyes y sistemas de denuncia, pero sin un conocimiento generalizado, siguen siendo infrautilizados. Recomienda ampliar las políticas educativas, dirigidas al profesorado, las poblaciones vulnerables y las personas mayores. A nivel regional, sugiere crear grupos de colaboración para promover estrategias compartidas en América Latina, adaptadas a las realidades locales, en lugar de replicar los marcos europeos.
	Nombre y cargo	**Derechos digitales**	**Protección de datos**	**Ciberdelincuencia**	**Buenas prácticas**	**Recomendaciones**

MEXICO	**Alfredo Sánchez** Abogado, litigante y especialista en derecho digital, actualmente director de Abogados Cibernéticos . Ha impartido docencia en Derecho de las Tecnologías de la Información en diversas universidades, centrando su carrera en litigios, investigación académica y reformas legislativas. Ha participado activamente en debates sobre ciberdelincuencia, derechos digitales y protección de datos. Su experiencia abarca la regulación de la IA, los derechos de autor en tecnologías emergentes y las lagunas procesales en la persecución de ciberdelitos.	México se basa en una Carta de Derechos Digitales no vinculante (de carácter meramente recomendatorio), lo que amplía la brecha persistente entre la política escrita y los derechos exigibles en la práctica. Las leyes fundamentales (LFPDPPP para el sector privado y LGPDPPSO para los organismos públicos) requieren una modernización urgente para reflejar la inteligencia artificial, la biometría, los neuroderechos y los usos contemporáneos de los datos. El estancamiento político, la falta de consenso y la débil capacidad institucional obstaculizan gravemente la protección eficaz y sostenible de los derechos humanos.	Las leyes de protección de datos heredadas, redactadas hace más de una década, funcionaron adecuadamente en su momento, pero ahora están rezagadas respecto a las cambiantes realidades tecnológicas y sociales. Las reformas deben incorporar inteligencia artificial, biometría, neuroderechos y una aplicación explícita de las mismas con principios, derechos y sanciones actualizados. A pesar de las múltiples propuestas académicas, no se ha promulgado ninguna actualización integral. La Corte Suprema está revisando la autoría de la IA y las implicaciones de los derechos de autor. La cultura de cumplimiento normativo es débil, y las autoridades técnicas facultadas siguen siendo insuficientemente eficaces y carecen de fondos suficientes.	Existe una policía cibernética a nivel federal y estatal, pero no existe un servicio de procesamiento especializado ni protocolos forenses establecidos para la cadena de custodia. Esta brecha procesal paraliza constantemente las investigaciones y socava la credibilidad de la fiscalía en todas las jurisdicciones. Solo el artículo 218 Bis C del Código Penal de Sinaloa tipifica como delito la manipulación dañina de imágenes mediante IA (las sanciones siguen siendo poco disuasorias contra la reincidencia). Un caso reciente de ciberdelito en la Ciudad de México fracasó por completo debido a la insuficiencia de herramientas, procedimientos y especialización institucional de investigación.	México cuenta con múltiples proyectos de ley relacionados con la IA en debate legislativo, aunque persisten disputas conceptuales y desacuerdos políticos. Las unidades de ciberpolicía ofrecen una primera respuesta y mantienen contacto directo con el público, ofreciendo campañas de concientización y prevención contra las amenazas digitales. La Suprema Corte validó el enfoque de Sinaloa sobre el uso indebido de la IA y está examinando cuestiones de derechos de autor. Existen avances aislados (capacitación en evidencia digital y propuestas de IA), pero siguen siendo limitados sin estándares nacionales armonizados ni un sistema de procesamiento nacional especializado.	Modernizar los marcos penales y de protección de datos (incluyendo explícitamente la IA, la biometría y los neuroderechos). Crear una agencia nacional de persecución penal de delitos cibernéticos con capacidad forense, protocolos estandarizados de evidencia y capacitación continua. Aumentar proporcionalmente las sanciones para los abusos facilitados por la IA donde la disuasión es baja. Evitar la copia y pega de documentos europeos sin fundamento crítico; adoptar soluciones adaptadas al contexto y culturalmente relevantes. Promover la cooperación regional en América Latina mediante códigos éticos compartidos, procedimientos interoperables y grupos de trabajo coordinados.
	Nombre y cargo	**Derechos digitales**	**Protección de datos**	**Ciberdelincuencia**	**Buenas prácticas**	**Recomendaciones**

MEXICO	**José Heriberto García Peña** Profesor-Investigador del Tecnológico de Monterrey (Campus Santa Fe) y Vicepresidente de Investigación e Innovación de FIADI. También es Director de la Revista Informática y Derecho. Desde 2006, se ha especializado en derecho de las TIC, protección de datos y ciberdelincuencia, contribuyendo a debates académicos, diálogos sobre políticas públicas y redes internacionales que promueven los derechos digitales en América Latina.	México ha avanzado en materia de derechos digitales, pero enfrenta retrocesos debido a las reformas institucionales. El desmantelamiento del INAI como organismo autónomo debilitó la supervisión, transfiriendo competencias a las secretarías. Si bien existe el marco legal (basado en garantías constitucionales y leyes de protección de datos), su aplicación y la independencia se están erosionando. Esto socava la confianza ciudadana, especialmente en contextos de corrupción, lo que limita el ejercicio efectivo de los derechos digitales y la transparencia.	El marco de protección de datos de México, inicialmente sólido con su ley de 2010, ahora corre el riesgo de fragmentarse. Los cambios en las definiciones de "datos personales" y "datos sensibles" han suscitado inquietud, mientras que el debilitamiento de la estructura de supervisión reduce la rendición de cuentas. Si bien las empresas de sectores regulados, en particular el financiero, continúan implementando programas de cumplimiento, la ausencia de una autoridad sólida e independiente compromete la capacidad de los ciudadanos para hacer valer sus derechos y exigir un procesamiento responsable de sus datos.	La legislación sobre ciberdelitos en México está fragmentada, pero evoluciona. Los códigos penales incluyen disposiciones para diversos delitos cibernéticos, pero su aplicación sigue siendo inconsistente. Existen unidades especializadas, pero la coordinación y los recursos son limitados. Las estrategias preventivas son insuficientes en comparación con las medidas reactivas. Si bien se están debatiendo propuestas para una ley nacional de ciberseguridad, las tensiones políticas y la fragmentación institucional dificultan respuestas eficaces y unificadas al ransomware, el fraude impulsado por IA y el ciberdelito transnacional.	México ha fomentado la colaboración entre múltiples actores, con la participación de la academia, el sector privado y las ONG en diálogos sobre IA, ciberseguridad y protección de datos. Iniciativas como el espacio de pruebas regulatorio de la ANIA sobre IA y los diálogos organizados por el Tecnológico de Monterrey destacan la innovación y los debates éticos. Si bien su aplicación es desigual, estos espacios contribuyen a definir políticas futuras, a cerrar brechas entre la teoría y la práctica, y a integrar la transparencia y la rendición de cuentas en los debates regulatorios.	México debe fortalecer la independencia institucional en materia de protección de datos, garantizando la continuidad del legado del INAI. Debe acelerar la adopción de leyes de ciberseguridad e IA, priorizando la transparencia, la supervisión humana y las garantías éticas. El desarrollo de capacidades en las agencias de aplicación de la ley, junto con programas de concientización para empresas y ciudadanos, es crucial. La cooperación regional con sus pares latinoamericanos fortalecería la resiliencia ante los desafíos comunes, a la vez que reduciría la dependencia de modelos regulatorios europeos importados.

5. Hallazgo

Los resultados comparativos en Bolivia, México, República Dominicana, Chile, Argentina, Colombia y Brasil confirman que la importación regulatoria sin adaptación debilita la eficacia. Mientras Europa debate la regulación del mercado y la protección del consumidor, en América Latina urge prevenir el autoritarismo digital y cerrar las brechas estructurales de las instituciones débiles. Como subraya la UNESCO, las soluciones regionales deben ser sensibles al contexto y no pueden ser una copia exacta de los marcos europeos o estadounidenses.

- **Contextualización local.** Los entrevistados enfatizaron constantemente que adoptar modelos sin considerar la cultura política, la capacidad de aplicación de la ley y las realidades locales produce marcos que parecen modernos en teoría, pero que resultan ineficaces en la práctica. Por ejemplo, la ley de datos de estilo español de República Dominicana que requiere una actualización y los proyectos de ley de IA de Bolivia, que requieren de una antesala en protección de datos.
- **Protección de las minorías.** Los encuestados también advirtieron que la gobernanza digital debe incorporar la diversidad cultural y la protección de las minorías. Casos en Ecuador y Bolivia muestran cómo las comunidades indígenas denunciaron la invisibilidad de sus lenguas y narrativas en las plataformas digitales, contradiciendo los principios de pluralismo e inclusión. Una gobernanza eficaz no se mide únicamente por la sofisticación institucional, sino también por la visibilidad y protección que los grupos marginados obtienen en los entornos digitales.
- **Ética y cierres**. Si bien pocos países regulan directamente prácticas como los shutdowns o la opacidad algorítmica, los entrevistados destacaron que la censura desproporcionada, la moderación opaca de contenido y los cierres contradicen los valores democráticos y violan el derecho de acceso a la información. Incorporar salvaguardas contra los cierres arbitrarios y la discriminación algorítmica se consideró esencial para garantizar una esfera digital participativa e inclusiva.
- **Crítica y oportunidad**. Las recomendaciones de la UNESCO son valiosas, pero enfrentan desafíos en América Latina debido a su carácter no vinculante y a la necesidad de una firme voluntad política. No obstante, las entrevistas sugieren que la UNESCO ofrece una hoja de ruta para exigir mayor responsabilidad a las empresas tecnológicas de la región, impulsar los debates nacionales sobre IA y protección de datos, y garantizar la participación significativa de la sociedad civil. La oportunidad reside en transformar las directrices del derecho indicativo en normas vinculantes, adaptándolas a la fragilidad institucional.

Análisis comparativo

Se observaron tres convergencias en los siete países. En primer lugar, la importación normativa sin adaptación produce cumplimiento teórico, pero protección limitada en la práctica. La ley de estilo español de República Dominicana, el complejo régimen bifurcado de México y los borradores de IA de Bolivia, que presuponen una antesala de protección de datos, ilustran los riesgos. En segundo lugar, las brechas de capacidad debilitan las leyes en cada etapa, la ANPD necesita recursos en Brasil; la actualización de Argentina tiene ciertos retrasos en su desarrollo; México carece de especialización fiscal; República Dominicana y Bolivia carecen de cobertura nacional; la autoridad de Colombia enfrenta límites de independencia y jurisdicción; Chile debe coordinar nuevas agencias y la implementación eficaz de su nueva normativa, así como establecer el rol de la Autoridad de Protección de datos. En tercer lugar, el aumento gradual de la vigilancia y la toma de decisiones automatizada se están extendiendo más rápido que la supervisión en los siete contextos. Los entrevistados coincidieron en que el futuro digital de América Latina depende de una regulación adaptativa y basada en principios, autoridades independientes empoderadas, capacidad de ciberseguridad interoperable y una verdadera

conciencia pública. De lo contrario, la innovación amplificará la desigualdad y la gobernanza digital seguirá siendo aspiracional en lugar de transformadora.

Derechos digitales

Chile y Brasil han avanzado en garantías formales (las salvaguardias centradas en el ser humano de Chile, incluyendo los neuroderechos en la esfera constitucional; la orientación de derechos de Brasil integrada en las estrategias digitales recientes). Argentina y México se basan en marcos antiguos que no rigen por completo los servicios estatales plataformados actuales ni las implementaciones biométricas opacas. República Dominicana reconoce constitucionalmente la privacidad y la protección de datos; sin embargo, las personas enfrentan recursos judiciales lentos y vías administrativas limitadas. Las entrevistas de Colombia advirtieron sobre la identificación biométrica generalizada y los usos judiciales experimentales de la IA con una supervisión débil, lo que crea riesgos de legitimidad. Bolivia carece de un andamiaje integral de derechos digitales, por lo que la protección depende de demandas constitucionales generales con resultados desiguales. En todos los países, los entrevistados enfatizaron tres déficits: transparencia limitada para la vigilancia estatal y la toma de decisiones automatizada, escasas vías para una reparación oportuna y baja conciencia pública. Sin educación y rendición de cuentas específicas, los derechos digitales siguen siendo aspiracionales, especialmente para los usuarios rurales, las mujeres, los niños y las comunidades indígenas.

Protección de datos

La LGPD de Brasil y el funcionamiento de la ANPD fueron elogiados, aunque los entrevistados destacaron la insuficiencia de recursos y la necesidad de una mayor difusión pública para que los canales de denuncia y las iniciativas de sandbox se utilicen eficazmente. La ley argentina (25.326) es madura, pero requiere ser actualizada; los proyectos de modernización se estancaron, dejando brechas para la IA y la biometría. Chile superó un largo período de obsolescencia con una nueva ley y una autoridad próxima a establecerse; sin embargo, la coordinación con su consejo de transparencia y la agencia de ciberseguridad será crucial. México opera dos regímenes paralelos (sector privado y público), pero la aplicación y la aceptación ciudadana siguen siendo deficientes; la complejidad del cumplimiento se suma a la desigual capacidad institucional. República Dominicana importó el modelo español anterior al RGPD y luego tuvo dificultades para contar con una autoridad competente más allá de los datos crediticios, lo que obligó a los ciudadanos a recurrir a tribunales que brindan respuestas lentas. En Colombia, la autoridad reside en el ejecutivo y enfrenta desafíos jurisdiccionales cuando las plataformas no tienen domicilio local. Bolivia aún carece de una ley integral de protección de datos; los entrevistados sugirieron un modelo pragmático que aproveche los reguladores sectoriales existentes (banca, telecomunicaciones) mientras se construye una autoridad central. El consenso: adaptar los principios inspirados en el RGPD a la capacidad local, no al revés.

Ciberseguridad

Brasil y Chile se destacaron por sus arquitecturas robustas. Brasil integra una política nacional con la estrategia eCyber 2025 y un denso ecosistema CSIRT; la coordinación e interoperabilidad entre estados se consideraron la próxima frontera. El nuevo marco de Chile establece operadores de vital importancia, obligaciones de evaluación de riesgos, reporte de incidentes, controles certificados y sanciones significativas, lo cual fue citado por los entrevistados como un referente regional. Argentina impulsó protocolos de evidencia digital y participa en la Convención de Budapest, mejorando la asistencia transfronteriza. México mantiene unidades de policía cibernética federales y estatales, pero carece de un cuerpo fiscal especializado y protocolos estandarizados de cadena de custodia digital, lo que debilita las investigaciones. La respuesta cibernética de República Dominicana está centralizada en Santo Domingo; otras provincias enfrentan dificultades y los tribunales sufren grandes retrasos, esta situación en específico,

refleja la situación de otros países como Bolivia o Brasil, donde la respuesta a un tipo de ciberdelito puede varias en el proceso de respuesta, según la ciudad en la que se presente la denuncia y la capacitación del personal, ya que no existe una estandarización en la respuesta. Colombia reportó una maduración sectorial en seguridad y defensa; sin embargo, la transparencia es limitada y la institucionalización a largo plazo es incierta. Bolivia cuenta con unidades de patrullaje cibernético solo en La Paz, Cochabamba y Santa Cruz, lo que deja a otros departamentos expuestos. Los siete hicieron hincapié en el aumento de los deepfakes, el phishing, el robo de identidad y el ransomware, y pidieron la adhesión al tratado de Budapest, capacitación continua y financiación de la capacidad forense en los cuerpos policiales, fiscales y de investigación.

Inteligencia artificial

Brasil cuenta con el Plan Nacional de IA y un proyecto de ley en debate (PL 2338), con entrevistas que destacan el valor de las aportaciones de múltiples partes interesadas y el riesgo de dilución de las salvaguardas impulsada por la industria. Chile está legislando con un enfoque basado en el riesgo alineado con los principios de la UNESCO y la UE, mientras que los académicos presionan para que se implementen entornos sandbox previos al despliegue en sectores de alto riesgo como la policía y la justicia. El debate en Argentina es activo en universidades y tribunales, pero no se ha materializado una ley integral de IA, las preocupaciones incluyen la dependencia judicial de herramientas genéricas sin explicabilidad. México muestra fragmentación, las propuestas federales cuestionan el alcance y las definiciones, mientras que Sinaloa criminalizó los usos maliciosos de deepfakes en 2024. se hizo referencia a la Corte Suprema en los desafíos en torno a la IA y la autoría. República Dominicana aprobó una estrategia nacional de IA con pilares de gobernanza, habilidades, centros de datos e integración regional, pero los expertos advirtieron sobre la débil aplicación de la ley sin una autoridad de datos facultada. Colombia volvió a presentar un proyecto de ley gubernamental sobre IA que busca la etiqueta ciertos deepfakes como de bajo riesgo, lo que generó críticas debido a los daños basados en el género. Los proyectos de ley de Bolivia no cuentan con una base adecuada referente al tratamiento de datos, lo cual quita la fuerza y utilidad a este tipo de nor as, lo que ilustra una falta de alineación entre la ambición y la realidad institucional.

Buenas prácticas

La gobernanza multisectorial de Brasil (CGI.br), las consultas públicas (FALA.br) y las iniciativas de la ANPD (canales de denuncia, sandbox) fueron citadas repetidamente como mecanismos inclusivos que convierten la ley en práctica. La ley de ciberseguridad de Chile operacionaliza la rendición de cuentas de operadores de vital importancia y sus salvaguardas constitucionales de integridad humana la posicionan a la vanguardia de los debates sobre tecnología y derechos humanos. La adhesión de Argentina a al convenio de Budapest y a los protocolos judiciales para evidencia digital fortalecen los enjuiciamientos y la cooperación. La reforma de Sinaloa en México es una respuesta a nivel estatal a la violencia de género habilitada por IA y los deepfakes, imperfecta pero catalizadora para el debate nacional; también se destacó la participación de la Corte Suprema en IA y autoría. La estrategia nacional de IA de República Dominicana y las estructuras centralizadas de ciberseguridad proporcionan un punto de partida para la gobernanza, incluso si la cobertura provincial es rezagada. La autoridad de datos de Colombia ha emitido una guía práctica sobre DPIA y cumplimiento para organismos públicos, y el poder judicial ha comenzado a discutir estándares de uso de IA. En Bolivia, los reguladores sectoriales (banca, telecomunicaciones) ya aplican controles estilo ISO, ofreciendo vías incrementales mientras se construyen leyes integrales.

Contribuciones y enfoque regional

Este análisis destaca que América Latina tiene la oportunidad de construir sus propios marcos de gobernanza tecnológica. Países como Chile, Brasil y Uruguay han dado pasos decisivos en materia de políticas de IA, pero la región en su conjunto debe fortalecer sus capacidades y reducir las disparidades. La intersección de la IA, la protección de datos y el cibercrimen exige políticas integrales y colaborativas que equilibren la innovación con los derechos. Adoptar un enfoque del Sur Global implica no depender de modelos externos, sino adaptar los principios internacionales a las realidades locales mediante la inclusión de comunidades históricamente excluidas.

Riesgos de la dependencia regulatoria

La replicación acrítica del RGPD o de la Ley de IA puede resultar en marcos que no se ajusten a las capacidades regionales. El proyecto de ley de IA de Brasil ejemplifica la tendencia a importar el modelo europeo, y el análisis de Access Now revela que muchas propuestas adoptan clasificaciones de niveles de riesgo sin adaptarse a los contextos locales [26]. Depender de estos modelos puede reforzar la dependencia tecnológica y la colonialidad digital. Por lo tanto, se recomienda un enfoque crítico y adaptativo que integre los estándares globales con las necesidades locales.

Recomendaciones

Para Bolivia, promulgar una ley de protección de datos adaptada al contexto que coordine a los reguladores del sector, modernizar las disposiciones sobre ciberdelitos, crear unidades judiciales y de procesamiento especializadas en todo el país, adherirse al convenio de Budapest. Para México, estandarizar la investigación forense digital y la cadena de custodia, crear una fiscalía nacional especializada y aclarar las normas de IA más allá de las reformas estatales aisladas, así como lineamientos de sanción de ciberdelitos. Para República Dominicana, establecer una autoridad de protección de datos independiente con alcance nacional, actualizar la ley de ciberdelitos, descentralizar la respuesta a incidentes y financiar la capacitación judicial para reducir la acumulación de casos. Para Chile, priorizar la coordinación interinstitucional para evitar la superposición de mandatos cuando la autoridad de datos esté operativa. Para Argentina, aprobar la reforma de la ley de protección de datos y continuar fortaleciendo la práctica de la evidencia digital. Para Colombia, reforzar la independencia y el alcance jurisdiccional de la autoridad de datos y regular las implementaciones biométricas con salvaguardas de derechos. Para Brasil, financiar adecuadamente la ANPD, cerrar las brechas de interoperabilidad y garantizar que la legislación sobre IA preserve los derechos, así como generar mayor difusión de las herramientas con las que cuentan actualmente. A nivel regional, todos instaron a leyes basadas en principios y adaptables, al desarrollo continuo de capacidades y a la alfabetización pública para que los mecanismos de queja y reparación se utilicen eficazmente.

Urgencia de un enfoque basado en derechos y centrado en la equidad

La gobernanza de la IA, la protección de datos y la ciberdelincuencia debe priorizar los derechos humanos, la equidad y la sostenibilidad. ILIA advierte que la IA puede impulsar el desarrollo o profundizar las desigualdades. GIRAI destaca que la mayoría de los países carecen de principios responsables de IA y políticas con perspectiva de género [27]. Por lo tanto, las

[26] Franco Giandana Gigena. (2024, 12 de marzo). ¿Cómo regula la Inteligencia Artificial América Latina? Accede ahora. https://www.accessnow.org/reporte-como-estamos-regulando-la-inteligencia-artificial-en-america-latina/

[27] La gobernanza de la IA no cumple con sus objetivos: el Índice Global de IA Responsable revela deficiencias críticas. (2024). Globalcenter.ai. https://www.globalcenter.ai/news/ai-governance-fails-to-deliver-global-index-on-responsible-ai-reveals-critical-gaps

políticas públicas deben incorporar mecanismos de transparencia, rendición de cuentas y evaluación del impacto social y ambiental. Solo mediante una gobernanza basada en derechos y adaptada a las particularidades regionales se puede aprovechar el potencial de la IA, protegiendo al mismo tiempo los datos personales y combatiendo la ciberdelincuencia sin sacrificar la justicia social ni la democracia.

Esto deja claro que los derechos no pueden adaptarse tras la experimentación regulatoria, más bien, deben integrarse desde la fase de diseño. Mecanismos como la transparencia, la rendición de cuentas, las evaluaciones de impacto y las garantías de equidad deben convertirse en elementos básicos de las políticas públicas. Solo mediante una gobernanza basada en derechos adaptada a las particularidades regionales se puede aprovechar el potencial transformador de las tecnologías emergentes sin socavar la democracia, la justicia social ni la dignidad humana.

Propuestas de políticas públicas específicas

Directrices generales

Las entrevistas y la revisión comparativa sugieren cinco principios rectores para el diseño regulatorio futuro en la región:

1. Regulación basada en riesgos adaptada a los contextos de IA, datos y ciberdelitos.
2. Cláusulas de revisión periódica y evaluaciones de impacto para garantizar la adaptabilidad.
3. Explicabilidad algorítmica, complementadas con auditorías independientes y evaluaciones obligatorias del impacto en la privacidad.
4. Participación multisectorial (Estado, sector privado, academia y sociedad civil) a lo largo de todo el ciclo regulatorio.
5. Armonización regional mediante normas compartidas, acuerdos de adecuación y fortalecimiento de la cooperación internacional.

Además, los gobiernos deben invertir en alfabetización digital, desarrollo de talentos y capacidad institucional para que estos marcos sean operativos.

6. Conclusiones y recomendaciones

Perspectivas desde las perspectivas locales y globales del Sur

Las entrevistas realizadas en Bolivia, México, República Dominicana, Chile, Argentina, Colombia y Brasil revelan una paradoja estructural, si bien algunos países han logrado impulsar marcos robustos (la LGPD de Brasil, la ley de ciberseguridad de Chile, la adhesión de Argentina al Convenio de Budapest), otros permanecen atrapados en modelos parciales o desactualizados. Desde una perspectiva del Sur Global, esta paradoja no es accidental, sino sintomática de un problema más profundo, la falta de contextualización. La regulación que ignora la economía política de los estados frágiles, el peso de la desigualdad o las limitaciones de las instituciones con fondos insuficientes se convierte en poco más que tinta simbólica sobre papel. Lo que emerge de las voces de los expertos locales es un poderoso reconocimiento de que la gobernanza adaptativa no es un floreo retórico, sino una estrategia de supervivencia para las sociedades que navegan por la volatilidad, la asimetría y la exclusión arraigada.

Riesgos de la dependencia normativa

Una lección central de este estudio es el peligro de la dependencia normativa. La implantación acrítica de modelos europeos (principalmente el RGPD y la Ley de IA) en contextos

latinoamericanos produce arquitecturas de cumplimiento que parecen sofisticadas en teoría, pero fracasan en la práctica. Los entrevistados describieron cómo obligaciones como la de los Delegados de Protección de Datos obligatorios abruman a pequeñas organizaciones sin presupuesto ni experiencia, a la vez que dejan sin regular dominios enteros donde faltan los prerrequisitos básicos. El proyecto de ley de IA de Bolivia, que no cuenta con una base legal previa en regulación relativa a entornos digitales. Esta dependencia corroe la credibilidad institucional, erosiona la confianza pública y perpetúa la colonialidad tecnológica. La alternativa no es el aislacionismo, sino la cocreación: marcos que se inspiran en estándares internacionales (RGPD, ética de IA de la UNESCO, principios de la OCDE), pero que se recalibran según la capacidad local, la cultura de aplicación y la realidad sociopolítica. Solo estos estándares adaptativos pueden evitar el doble peligro de la sobrerregulación sin implementación y la subregulación sin rendición de cuentas.

Urgencia de una gobernanza tecnológica centrada en los derechos

El futuro digital de América Latina y el Caribe depende de si los derechos se sitúan en el epicentro de la gobernanza tecnológica. La región no puede permitirse una regulación reactiva o fragmentada, ni puede apostar por agendas impulsadas externamente que ignoren las realidades sociales. En cambio, tres prioridades urgentes se cristalizan tanto en las entrevistas como en el análisis comparativo:

1) El establecimiento de autoridades independientes, con recursos suficientes y políticamente protegidas, capaces de garantizar la protección de datos, la ciberseguridad y la supervisión de la IA. Sin independencia ni recursos, incluso las leyes más avanzadas permanecen inertes.
2) La construcción de la alfabetización social en torno a la tecnología y los derechos. Las leyes sin conciencia ciudadana se vuelven performativas; los ciudadanos deben comprender sus derechos para poder ejercerlos. Por lo tanto, la alfabetización digital, la transparencia y los mecanismos participativos de rendición de cuentas no son secundarios, sino fundamentales.
3) Coordinación regional para superar la fragmentación. Sin estándares transfronterizos, cooperación regional en ciberseguridad y acuerdos de adecuación compartidos, América Latina y el Caribe corre el riesgo de seguir siendo un mosaico de regímenes desconectados, vulnerable tanto al control corporativo como al uso indebido autoritario de las herramientas digitales.

Una encrucijada regional

Los hallazgos de este estudio dejan claro lo que está en juego, América Latina y el Caribe se encuentran en una encrucijada donde dos futuros divergen. Un futuro se define por la dependencia, la fragmentación y las leyes simbólicas que reproducen la desigualdad y la subordinación tecnológica. El otro futuro se define por una gobernanza adaptativa, participativa y orientada a la equidad que convierte las tecnologías disruptivas en auténticos instrumentos de democracia y justicia social.

Optar por esto último requiere valentía, abandonar la comodidad de los patrones importados, reconocer la especificidad de las realidades regionales e integrar los derechos no como anexos decorativos, sino como la arquitectura central de la regulación. Los derechos no pueden incorporarse posteriormente a la promulgación de las leyes, deben estar presentes desde la fase de diseño. Los mecanismos de transparencia, rendición de cuentas, evaluación de impacto y salvaguardas de la equidad no son lujos, sino herramientas de supervivencia para las sociedades democráticas que enfrentan la disrupción tecnológica.

Llamado a la acción

Ya pasó la era de las medidas a medias. América Latina no puede permitirse ser un laboratorio pasivo de modelos externos ni un panorama fragmentado de regulaciones simbólicas. Los responsables políticos, los reguladores y la sociedad civil deben actuar colectivamente para crear una gobernanza adaptativa basada en los derechos, la equidad y la inclusión. Esto requiere invertir en capacidad institucional, desarrollar la alfabetización digital desde la base y forjar una cooperación regional que trascienda las declaraciones y se convierta en compromisos vinculantes. Los académicos y profesionales también deben ir más allá de la crítica, generando conocimiento práctico que cierre la brecha entre la ley y la realidad.

Si la región no actúa, la disrupción tecnológica intensificará la exclusión, la captura corporativa y el control autoritario. Pero si América Latina adopta una gobernanza adaptativa y centrada en los derechos, puede transformar las tecnologías disruptivas en una plataforma para la democracia, la justicia distributiva y el desarrollo sostenible. La responsabilidad es inmensa, pero también lo es la oportunidad: construir no solo leyes que regulen la tecnología, sino también marcos de gobernanza que definan un futuro digital más equitativo. El próximo capítulo de la gobernanza tecnológica global no se escribirá solo en Bruselas o Washington, también puede y debe, escribirse en América Latina.

Referencias bibliográficas

Access Now. (2024). Regulatory Mapping on Artificial Intelligence in Latin America. https://www.accessnow.org/publication/regulatory-mapping-on-artificial-intelligence-in-latin-america/

AI Governance Fails to Deliver: Global Index on Responsible AI Reveals Critical Gaps. (2024). Globalcenter.ai. https://www.globalcenter.ai/news/ai-governance-fails-to-deliver-global-index-on-responsible-ai-reveals-critical-gaps

ANPD (Autoridade Nacional de Proteção de Dados). (2024, November 29). Preliminary Study on Generative AI. https://www.fpf.org/blog/brazils-anpd-preliminary-study-on-generative-ai-highlights-the-dual-nature-of-data-protection-law-balancing-rights-with-technological-innovation/

Chile's New Data Protection Law: Context, Overview, and Key Takeaways. (2025, February 27). FPF. https://fpf.org/blog/chiles-new-data-protection-law-context-overview-and-key-takeaways

Chile – Data Protection and Cybersecurity Laws. (2025). CMS Expert Guide. https://cms.law/en/int/expert-guides/cms-expert-guide-to-data-protection-and-cyber-security-laws/chile?format=pdf&v=3

Codigo Penal Bolivia Libro Primero Parte General Título I La Ley Penal Capítulo Único Reglas Para Su Aplicación. (N.D.). Https://Www.Oas.Org/Juridico/Spanish/Gapeca_Sp_Docs_Bol1.Pdf

Consejo Nacional de Inteligencia Artificial (CENIA). (2024). ILIA 2024: Latin American Artificial Intelligence Index. CEPAL. https://www.cepal.org/en/notes/ilia-2024-evaluating-ai-readiness-and-progress-latin-america

DLA Piper. (2024). Data protection laws in Brazil — In force since September 18, 2020, the Brazilian General Data Protection Law (LGPD). https://www.dlapiperdataprotection.com/index.html?c=BR&t=law

Economic Commission for Latin America and the Caribbean & National Center for Artificial Intelligence (CENIA). (2024, October 7). Latin American Artificial Intelligence Index (ILIA 2024):

Evaluating AI Readiness and Progress in Latin America. https://www.cepal.org/en/notes/ilia-2024-evaluating-ai-readiness-and-progress-latin-america

Economic Commission for Latin America and the Caribbean (ECLAC). (2024, September 24). Latin American Artificial Intelligence Index (ILIA) reconfirms Chile, Brazil and Uruguay as leaders in the region. CEPAL. https://www.cepal.org/en/pressreleases/latin-american-artificial-intelligence-index-ilia-reconfirms-chile-brazil-and-uruguay

Fortra. (2025, July 27). Cybersecurity regulatory landscape in Chile: A primer for businesses. https://www.fortra.com/blog/cybersecurity-regulatory-landscape-chile-primer-businesses

Franco Giandana Gigena. (2024, March 12). ¿Cómo regula la Inteligencia Artificial América Latina? Access Now. https://www.accessnow.org/reporte-como-estamos-regulando-la-inteligencia-artificial-en-america-latina/

Global Index on Responsible AI and Georgia's Results. (2024). Https://Idfi.ge/En. https://idfi.ge/en/global_center_on_ai_governance_2024

Government of Canada & United States Agency for International Development. (2024). Global Index on Responsible AI: Corrected Edition. Agata Data. https://agatadata.com/wp-content/uploads/2024/11/Global-Index-on-Responsible-AI-2024-Corrected-Edition-25_10_24-Gobierno-de-Canada-y-USAID.pdf

ILIA 2024: Evaluating AI Readiness and Progress in Latin America | CEPAL. (2024). Economic Commission for Latin America and the Caribbean. https://www.cepal.org/en/notes/ilia-2024-evaluating-ai-readiness-and-progress-latin-america

Latin American Artificial Intelligence Index (ILIA). (2024). ILIA 2024: Evaluating AI readiness and progress in Latin America. ECLAC / CENIA. https://www.cepal.org/en/notes/ilia-2024-evaluating-ai-readiness-and-progress-latin-america

Latin American Open Data Initiative (ILDA). EmpatIA: AI to solve public issues in LATAM. (2022-23). EmpatIA project description and policy briefings. ILDA. Paris Peace Forum

Latin American Data Privacy. (2025, January 28). Crowell & Moring: Country briefs on data protection. https://www.crowell.com/en/insights/publications/latin-american-data-privacy

Levy Yeyati, E. (2025, May 22). Smart AI regulation strategies for Latin American policymakers. Brookings Institution. https://www.brookings.edu/articles/smart-ai-regulation-strategies-for-latin-american-policymakers/

Observatory of Cybersecurity in Latin America and the Caribbean. (2025). Latin America & the Caribbean: Climbing the Cybersecurity Ladder. GFCE. https://www.thegfce.org/news/latin-america-and-the-caribbean-climbing-the-cybersecurity-ladder/

Overview of AI policy in 10 jurisdictions | Digital Watch Observatory. (2024, December 23). Digital Watch Observatory. https://dig.watch/updates/overview-of-ai-policy-in-10-jurisdictions

United Nations Economic Commission for Latin America and the Caribbean (ECLAC) & Centro Nacional de Inteligencia Artificial (CENIA). (2024). ILIA 2024: Evaluating AI Readiness and

Progress in Latin America.
https://www.cepal.org/en/notes/ilia-2024-evaluating-ai-readiness-and-progress-latin-america

Uruguay Digital. (2021). Agenda Uruguay Digital 2025. Gobierno de Uruguay.
https://dig.watch/resource/agenda-uruguay-digital-2025

West, D. M. (2024). Smart AI regulation: Strategies for Latin American policymakers. Brookings Institution.
https://www.brookings.edu/articles/smart-ai-regulation-strategies-for-latin-american-policymakers

White & Case. (2025, June 6). AI Watch: Global regulatory tracker – Brazil.
https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-brazil

Xenoss. (2023, October 27). AI regulation in Latin America (LATAM): Brazil leads. Xenoss Blog.
https://xenoss.io/blog/latin-america-latam-ai-regulations

Apéndice

Guía de Entrevista Semiestructurada

Proyecto: Gobernanza Tecnológica Adaptable: Hacia Políticas Públicas Flexibles para Tecnologías Disruptivas en América Latina y el Caribe

Introducción y Consentimiento

Antes de comenzar, quisiera pedir su consentimiento para grabar esta entrevista con fines estrictamente investigativos. El audio será transcrito para análisis cualitativo, y la información se usará únicamente en el marco del proyecto LACNIC 2025. ¿Está de acuerdo con la grabación de esta conversación?

¿Desea que su participación en el estudio sea identificada con su nombre, cargo y afiliación institucional, o prefiere mantenerse en el anonimato? En caso de aceptar ser identificado, ¿podría confirmar cómo desea que aparezcan su nombre completo, cargo actual y afiliación institucional en la investigación?

Trayectoria Profesional

- ¿Podría describir brevemente su trayectoria profesional y su campo de trabajo actual?

Derechos Digitales y Derechos Humanos

- ¿Cree que las regulaciones digitales actuales en su país incorporan adecuadamente una perspectiva de derechos humanos? ¿Por qué sí o por qué no?

Instituciones y Capacidades

- ¿Qué instituciones lideran actualmente los procesos relacionados con protección de datos, ciberseguridad o inteligencia artificial en su país?
- En su opinión, ¿estas instituciones cuentan con la capacidad técnica, financiera y política suficiente para implementar y supervisar de manera efectiva los marcos de derechos digitales?

Protección de Datos

- ¿Cómo evalúa el desarrollo del marco legal sobre protección de datos personales en su país?
- ¿Considera que las leyes de protección de datos existentes son adecuadas para abordar los desafíos actuales y emergentes, como el uso de biometría, el procesamiento de datos mediante IA o los flujos transfronterizos de datos?

Ciberdelitos y Ciberseguridad

- ¿Cuál es su percepción de la legislación vigente sobre ciberdelitos en su país?
- ¿Existen códigos penales actualizados, procedimientos de investigación o unidades especializadas que aborden de manera efectiva los ciberdelitos y la ciberseguridad?

Regulación de Inteligencia Artificial

- ¿Conoce alguna iniciativa legislativa o de políticas públicas sobre inteligencia artificial en su país?
- En caso afirmativo, ¿estas iniciativas incluyen salvaguardas como transparencia, rendición de cuentas, supervisión humana y protección de los derechos fundamentales?

Alineación y Contexto

- En su opinión, ¿las regulaciones sobre derechos digitales, protección de datos e IA han sido diseñadas para responder a las realidades específicas de su país o replican principalmente modelos externos (como el RGPD o el AI Act de la UE) sin suficiente adaptación a los contextos locales?

Recomendaciones Personales

- Con base en su experiencia, ¿qué recomendaciones haría a legisladores, reguladores o responsables de políticas públicas para mejorar el diseño e implementación de las regulaciones sobre protección de datos, ciberdelitos, IA y derechos digitales?
- ¿Qué tecnologías emergentes o riesgos (por ejemplo, IA generativa, neurotecnología, computación cuántica) deberían priorizarse en los futuros marcos de gobernanza?