DIPUTADOS
ARGENTINA

PROYECTO DE LEY

EL SENADO Y CÁMARA DE DIPUTADOS DE LA NACIÓN ARGENTINA, REUNIDOS EN CONGRESO, SANCIONAN CON FUERZA DE LEY:

RÉGIMEN FEDERAL DE ADMISIBILIDAD Y VALORACIÓN DE PRUEBA DIGITAL Y EVIDENCIA TECNOLÓGICA EN PROCESOS JUDICIALES Y ADMINISTRATIVOS

ARTÍCULO 1° — OBJETO

La presente ley tiene por objeto establecer un régimen legal uniforme para la admisión, producción, valoración, conservación y control de la prueba digital y de la evidencia tecnológica en los procesos judiciales y administrativos, garantizando seguridad jurídica, debido proceso, defensa en juicio y control jurisdiccional efectivo.

ARTÍCULO 2° — ÁMBITO DE APLICACIÓN

Las disposiciones de la presente ley son aplicables a:

a) Los procesos judiciales de competencia federal;

b) Los procedimientos administrativos tramitados ante la Administración Pública Nacional y entes reguladores nacionales, cuando produzcan efectos sancionatorios o patrimoniales;

c) Los procesos judiciales provinciales y de la Ciudad Autónoma de Buenos Aires que adhieran expresamente a la presente ley mediante legislación local.

Sin perjuicio de la autonomía procesal local, los principios de esta ley relativos a defensa en juicio, contradicción, acceso a la evidencia y control pericial constituyen estándares interpretativos compatibles con el artículo 18 de la Constitución Nacional.

TÍTULO I

CONCEPTO Y CLASIFICACIÓN DE LA PRUEBA DIGITAL

ARTÍCULO 3° — DEFINICIÓN

Se considera prueba digital a toda información con relevancia jurídica generada, almacenada, transmitida o verificada mediante sistemas informáticos, tecnologías de registros distribuidos, medios criptográficos, inteligencia artificial u otras tecnologías digitales emergentes, susceptible de ser incorporada válidamente a un proceso.

ARTÍCULO 3° bis — APLICACIÓN SUPLETORIA

Los documentos electrónicos y comunicaciones digitales regulados por los códigos procesales vigentes se rigen por sus normas específicas. No obstante, los principios de integridad, autenticidad, trazabilidad, preservación y contradicción establecidos en la presente ley podrán aplicarse supletoriamente cuando resulten pertinentes por la naturaleza técnica del caso.

ARTÍCULO 4° — CATEGORÍAS DE PRUEBA DIGITAL

Constituyen prueba digital regulada por esta ley, entre otras:

a) Registros generados en tecnologías de registros distribuidos (blockchain o DLT);

b) Logs criptográficos y registros de eventos informáticos;

c) Hashes, sellos de tiempo digitales y huellas criptográficas;

d) Registros de sistemas automatizados o contratos inteligentes;

e) Resultados producidos por sistemas de inteligencia artificial explicable;

f) Metadatos asociados a documentos digitales;

g) Evidencia digital forense extraída conforme a protocolos técnicos reconocidos.

TÍTULO II

ADMISIBILIDAD Y VALOR PROBATORIO

ARTÍCULO 5° — PRINCIPIO DE EQUIVALENCIA FUNCIONAL

La prueba digital no podrá ser rechazada ni privada de efectos jurídicos por el solo hecho de su naturaleza tecnológica, siempre que cumpla con los requisitos de autenticidad, integridad, trazabilidad y posibilidad de contradicción.

ARTÍCULO 6° — REGISTROS BLOCKCHAIN

Los registros generados en tecnologías blockchain o DLT constituyen principio de prueba y podrán adquirir plena fuerza probatoria cuando:

a) Sea técnicamente verificable su integridad;

b) Exista correspondencia razonable entre el registro y el hecho invocado;

c) Se garantice la posibilidad de control pericial y contradicción.

A los efectos del control pericial, quien invoque el registro deberá identificar, en la medida de lo razonablemente posible, la red o sistema utilizado, el identificador de transacción o registro (TXID u equivalente), el bloque o altura (cuando corresponda), y el hash vinculado al contenido cuya integridad se pretende acreditar.

El juez valorará su eficacia conforme a las reglas de la sana crítica racional.

ARTÍCULO 6° bis — LÍMITES PROBATORIOS DEL REGISTRO BLOCKCHAIN

Los registros blockchain acreditan:

a) La existencia de información en un momento determinado;

b) La integridad de esa información desde su registro;

c) La secuencia cronológica de transacciones en la cadena.

No acreditan por sí solos:

a) La veracidad del contenido registrado;

b) La identidad real de las partes, salvo vinculación verificable con sistemas de

identificación confiables;

c) Hechos del mundo físico, sin medios de verificación complementarios.

El valor probatorio del contenido depende de otros medios que acrediten su correspondencia con la realidad.

ARTÍCULO 7° — LOGS, HASHES Y SELLOS DE TIEMPO

Los logs criptográficos, hashes y sellos de tiempo digitales constituyen medios idóneos para acreditar:

a) Existencia de un archivo o mensaje en un momento determinado;

b) Integridad y no alteración de la información;

c) Secuencia temporal de eventos digitales.

ARTÍCULO 7° bis — VALOR PROBATORIO DE METADATOS

Los metadatos asociados a archivos digitales (fecha de creación, modificación, autoría, geolocalización, dispositivo de origen) constituyen medios de prueba sobre las circunstancias de generación del contenido.

Su valor probatorio se apreciará conforme a:

a) Posibilidad técnica de alteración;

b) Coherencia con otros elementos probatorios;

c) Nivel de protección técnica del sistema de origen;

d) Certificación por terceros confiables cuando exista.

TÍTULO III

INTELIGENCIA ARTIFICIAL COMO MEDIO DE PRUEBA

ARTÍCULO 8° — IA EXPLICABLE

Los resultados producidos por sistemas de inteligencia artificial podrán ser ofrecidos como medio de prueba cuando el sistema permita:

a) Explicar de manera comprensible para un perito técnico independiente los criterios generales de funcionamiento, las variables principales utilizadas y, cuando sea técnicamente posible, el peso relativo de aquellas en el resultado, mediante documentación técnica y métodos de explicabilidad reconocidos;

b) Identificar las variables relevantes utilizadas;

c) Permitir su evaluación pericial independiente.

No podrán admitirse como prueba exclusiva sistemas cuya lógica sea absolutamente opaca o no auditable, cuando ello impida la contradicción efectiva.

La evaluación pericial podrá realizarse bajo medidas de confidencialidad razonables para proteger secretos comerciales, datos personales o información sensible, incluyendo exhibición limitada, revisión en sede judicial (in camera) y acuerdos de confidencialidad para peritos y consultores técnicos.

ARTÍCULO 9° — VALORACIÓN JUDICIAL

El juez no podrá delegar la decisión jurisdiccional en sistemas automatizados.

La inteligencia artificial constituye auxilio probatorio, no órgano decisor.

TÍTULO IV

CARGA PROBATORIA, PRESERVACIÓN Y DISPONIBILIDAD DE LA EVIDENCIA

ARTÍCULO 10° — PRINCIPIO DE DISPONIBILIDAD TECNOLÓGICA

Cuando una de las partes se encuentre en mejor posición técnica, económica o informativa para producir o conservar la prueba digital, el juez podrá aplicar criterios de carga probatoria dinámica, fundando expresamente su decisión.

ARTÍCULO 11° — DEBER DE CONSERVACIÓN

Quien controle sistemas digitales relevantes para una controversia deberá preservar la evidencia digital razonablemente previsible, bajo apercibimiento de presunción adversa en caso de destrucción o alteración injustificada.

ARTÍCULO 11° bis — DESTRUCCIÓN DE EVIDENCIA DIGITAL (SPOLIATION)

La destrucción, alteración u ocultamiento intencional o gravemente negligente de evidencia digital relevante genera:

a) Presunción judicial adversa respecto del contenido destruido, presumiéndose que era desfavorable a quien la destruyó;

b) Posibilidad de inversión de la carga probatoria;

c) Valoración negativa de conducta procesal conforme al artículo 34 inciso 5° del Código Procesal Civil y Comercial de la Nación o normas equivalentes;

d) Responsabilidad por costas y por los perjuicios causados conforme a las reglas generales aplicables, cuando corresponda.

El deber de conservación nace cuando:

a) Se inicia formalmente el proceso;

b) Se notifica requerimiento extrajudicial fehaciente;

c) Es razonablemente previsible el litigio por la naturaleza del conflicto.

No hay destrucción culpable cuando obedece a:

a) Políticas ordinarias de retención de datos aplicadas consistentemente antes del conflicto;

b) Imposibilidad técnica o costo desproporcionado de conservación;

c) Cumplimiento de obligaciones legales de eliminación de datos.

La preservación deberá ser proporcional y compatible con la normativa de protección de datos personales, pudiendo disponerse medidas de minimización, seudonimización o resguardo bajo confidencialidad cuando resulte necesario.

ARTÍCULO 11° ter — MEDIDAS URGENTES DE PRESERVACIÓN (LEGAL HOLD)

A pedido de parte y con verosimilitud del derecho, el juez podrá ordenar medidas urgentes de preservación de evidencia digital, incluyendo la conservación de logs, copias forenses, respaldos, contenidos alojados en la nube y datos en poder de terceros, bajo apercibimiento de astreintes y demás medidas compulsorias aplicables.

Cuando la medida pueda afectar derechos de terceros o información sensible, el juez podrá disponer modalidades de preservación bajo confidencialidad, custodia judicial o depósito técnico.

TÍTULO V

CADENA DE CUSTODIA DIGITAL

ARTÍCULO 12° — PRINCIPIO DE TRAZABILIDAD

Toda evidencia digital deberá mantener una cadena de custodia documentada que permita verificar:

a) Origen;

b) Método de obtención;

c) Conservación;

d) Accesos;

e) Eventuales transformaciones técnicas.

ARTÍCULO 13° — ALTERACIONES Y COPIAS

La existencia de copias técnicas o transformaciones necesarias para el análisis pericial

no invalida la prueba si se conserva la trazabilidad y verificabilidad del original digital.

ARTÍCULO 13° bis — ESTÁNDARES Y PROTOCOLOS DE REFERENCIA

La autoridad de aplicación elaborará, en coordinación con organismos técnicos competentes y con el Poder Judicial de la Nación, estándares técnicos de referencia para cadena de custodia digital, documentación y verificación criptográfica.

Su adopción operativa en la jurisdicción federal se instrumentará conforme las acordadas y reglamentos del Poder Judicial de la Nación, sin perjuicio de la adhesión provincial.

Hasta tanto se establezcan dichos estándares, podrán utilizarse como referencia estándares internacionales reconocidos (ISO/IEC 27037, NIST SP 800-86, RFC 3227, o sus actualizaciones vigentes).

ARTÍCULO 13° ter — PRODUCCIÓN EN FORMATO NATIVO

Cuando sea técnicamente razonable, la prueba digital deberá producirse en su formato nativo preservando metadatos relevantes, a fin de asegurar integridad, trazabilidad y control pericial.

Si por motivos fundados de confidencialidad o seguridad no fuera posible producirla en formato nativo, el juez podrá autorizar formatos alternativos siempre que se preserve la verificabilidad mediante hash u otros medios técnicos idóneos.

TÍTULO VI

PERICIA TECNOLÓGICA

ARTÍCULO 14° — PERITOS ESPECIALIZADOS

Cuando la prueba digital lo requiera, el juez deberá designar peritos con formación específica en informática forense, criptografía, ciencia de datos o tecnologías pertinentes al caso.

ARTÍCULO 14° bis — REGISTRO Y FORMACIÓN DE PERITOS

En el ámbito de la Justicia Nacional y Federal, el Poder Judicial creará un Registro de

Peritos en Tecnologías Digitales, estableciendo requisitos de formación, certificación y actualización continua.

Podrán inscribirse:

a) Profesionales con título universitario en informática, ingeniería en sistemas, matemática aplicada o carreras afines;

b) Quienes acrediten formación de posgrado específica en las materias de esta ley;

c) Peritos certificados internacionalmente en informática forense u otras certificaciones reconocidas.

En casos de alta complejidad o escasez de peritos, los tribunales podrán designar peritos de otras jurisdicciones, instituciones técnicas especializadas, o peritos internacionales, bajo reglas de idoneidad y contradicción.

ARTÍCULO 15° — CONTRADICCIÓN, AUDITORÍA Y GARANTÍAS DE DEFENSA

Las partes tienen derecho a:

a) Acceder a copias forenses completas de la evidencia digital, en formatos técnicamente accesibles, salvo restricciones fundadas;

b) Controlar el trabajo pericial en todas sus etapas, mediante notificaciones previas de cada actuación relevante;

c) Designar consultores técnicos con acceso a la evidencia en igualdad de condiciones que el perito oficial;

d) Solicitar auditorías independientes cuando la complejidad técnica, el valor en disputa o la asimetría de recursos lo justifiquen;

e) Solicitar plazos razonables adecuados a la complejidad del análisis técnico requerido;

f) En casos de notorias asimetrías económicas que afecten el derecho de defensa, solicitar la designación de consultor técnico de oficio conforme las reglas aplicables.

El juez deberá garantizar efectivamente estos derechos. La inobservancia que cause indefensión concreta podrá dar lugar a la nulidad de la prueba o a su desestimación, sin perjuicio de asignarle menor valor probatorio conforme a la sana crítica.

TÍTULO VII

DISPOSICIONES COMPLEMENTARIAS

ARTÍCULO 16° — NORMAS SUPLETORIAS

En todo lo no previsto por esta ley, resultan aplicables las normas procesales vigentes y los principios generales del derecho probatorio.

ARTÍCULO 17° — CAPACITACIÓN JUDICIAL

El Poder Judicial de la Nación, en coordinación con el Poder Ejecutivo y las jurisdicciones provinciales adheridas, promoverá programas de capacitación continua en prueba digital y evidencia tecnológica para magistrados, funcionarios y auxiliares de justicia.

TÍTULO VIII

DISPOSICIONES FINALES Y TRANSITORIAS

ARTÍCULO 18° — PROCESOS EN TRÁMITE

La presente ley se aplicará a la prueba ofrecida, admitida o producida con posterioridad a su entrada en vigencia, aun en procesos iniciados con anterioridad, sin afectar prueba ya producida y valorada.

Las normas sobre conservación de evidencia (artículos 11, 11 bis y 11 ter) se aplicarán a hechos ocurridos con posterioridad a la entrada en vigencia de esta ley.

ARTÍCULO 19° — AUTORIDAD DE APLICACIÓN

El Ministerio de Justicia y Derechos Humanos de la Nación será autoridad de aplicación en coordinación con:

a) El Consejo de la Magistratura del Poder Judicial de la Nación;

b) El Poder Judicial de la Nación;

c) Las autoridades judiciales provinciales y de la Ciudad Autónoma de Buenos Aires que adhieran a la presente ley;

d) Organismos técnicos especializados, universidades nacionales y colegios profesionales, cuando corresponda.

La autoridad de aplicación no podrá dictar disposiciones que importen regulación de la valoración judicial de la prueba ni afectar la independencia funcional del Poder Judicial, limitándose a establecer estándares técnicos de referencia y mecanismos de cooperación interinstitucional.

ARTÍCULO 20° — REGLAMENTACIÓN

El Poder Ejecutivo reglamentará la presente ley dentro del plazo de CIENTO OCHENTA (180) días desde su promulgación, pudiendo establecer:

a) Estándares técnicos de referencia para cadena de custodia digital;

b) Requisitos de certificación y actualización de peritos y organismos de formación reconocidos;

c) Estándares mínimos de explicabilidad para sistemas de inteligencia artificial;

d) Procedimientos de interoperabilidad con registros judiciales electrónicos;

e) Modelos de documentación de cadena de custodia y formularios estandarizados;

f) Criterios de actualización periódica conforme a evolución tecnológica.

La reglamentación no podrá restringir garantías procesales ni establecer requisitos que impidan o dificulten irrazonablemente el acceso a la justicia.

ARTÍCULO 21° — CLÁUSULA DE REVISIÓN

El Congreso de la Nación procederá a la revisión integral de esta ley dentro del plazo de TRES (3) años desde su entrada en vigencia, considerando:

a) Evolución tecnológica y aparición de nuevas categorías de evidencia digital;

b) Jurisprudencia desarrollada por tribunales federales y de jurisdicciones adheridas;

c) Experiencia comparada internacional;

d) Informes de la autoridad de aplicación sobre dificultades de implementación;

e) Recomendaciones de organismos técnicos y académicos especializados.

ARTÍCULO 22° — VIGENCIA

La presente ley entrará en vigencia a los NOVENTA (90) días de su publicación en el Boletín Oficial.

ARTÍCULO 23° — COMUNÍQUESE AL PODER EJECUTIVO

LIC. MARCELA MARINA PAGANO
DIPUTADA DE LA NACIÓN

DIPUTADOS
ARGENTINA

FUNDAMENTOS (VERSIÓN DEFINITIVA)

Señor Presidente:

La presente iniciativa tiene por objeto dotar al sistema judicial y administrativo argentino de un marco normativo moderno, técnicamente informado y constitucionalmente sólido para la admisión, preservación, producción y valoración de prueba digital y evidencia tecnológica.

El sistema probatorio vigente fue diseñado para una realidad predominantemente analógica. Sin embargo, los hechos jurídicamente relevantes del siglo XXI —contratación digital, transacciones financieras, relaciones de consumo en plataformas, trabajo remoto, fraude informático, trazabilidad logística, registros distribuidos e inteligencia artificial— se producen y documentan mediante sistemas tecnológicos que hoy carecen de un estatuto probatorio uniforme y previsible.

En la práctica, los tribunales se ven forzados a resolver por analogía, con criterios dispares, generando incertidumbre jurídica, incremento de litigiosidad incidental y desigualdad real entre partes con capacidades técnicas y recursos económicos asimétricos.

I. OBJETIVOS

El proyecto persigue:

1. Establecer reglas claras de admisibilidad y valoración de nuevas categorías de evidencia (blockchain, logs criptográficos, hashes, metadatos, sistemas automatizados, IA explicable);

2. Asegurar debido proceso y contradicción efectiva en contextos tecnológicos complejos, garantizando el control pericial y el acceso a la evidencia;

3. Incorporar reglas de preservación de evidencia y tratamiento de la destrucción u ocultamiento de prueba (spoliation) compatibles con protección de datos y proporcionalidad;

4. Profesionalizar la pericia tecnológica mediante criterios de especialización, registro y auditoría;

5. Dotar al derecho argentino de herramientas procesales coherentes con la modernización del derecho privado y del comercio digital.

II. DISEÑO CONSTITUCIONAL Y FEDERAL

La ley se aplica directamente a:

- procesos de competencia federal, y
- procedimientos administrativos nacionales con efectos sancionatorios o patrimoniales.

Respecto de procesos provinciales, se prevé adhesión expresa, preservando la autonomía local. En paralelo, la norma establece principios compatibles con el artículo 18 de la Constitución Nacional (defensa, contradicción, acceso a evidencia), actuando como guía interpretativa sin pretender sustituir los códigos de forma provinciales.

Este diseño evita conflictos de competencia, pero asegura un núcleo de garantías procesales tecnológicamente adecuadas en el ámbito federal y en la administración pública nacional, con posibilidad de expansión federal cooperativa.

III. CONTENIDO INNOVADOR

El proyecto introduce, por primera vez de manera sistemática:

- Reconocimiento de registros blockchain/DLT como principio de prueba con criterios de verificabilidad y contradicción, incorporando límites expresos para evitar el error conceptual de asumir “veracidad” por el solo hecho del registro;
- Valor probatorio de logs criptográficos, hashes y sellos de tiempo;
- Estatuto probatorio de metadatos y su valoración conforme a posibilidad de alteración y coherencia probatoria;

- Admisibilidad condicionada de evidencia derivada de IA bajo estándares de explicabilidad y auditoría, protegiendo simultáneamente secretos comerciales mediante medidas de confidencialidad;

- Deber de preservación de evidencia y régimen de spoliation con efectos procesales claros y proporcionales;

- Medidas urgentes de preservación (“legal hold”) para evitar pérdida de evidencia en nube o en poder de terceros;

- Cadena de custodia digital con estándares de referencia y adopción operativa respetuosa de la independencia judicial.

IV. IMPACTO ESPERADO

La ley reducirá incidentes de admisibilidad y nulidades por defectos técnicos, incrementará previsibilidad en litigios de consumo, fintech y contratación digital, fortalecerá persecución y sanción de fraudes informáticos, y mejorará el estándar de prueba en el Estado y en la justicia, sin delegar función jurisdiccional ni automatizar decisiones.

V. CONCLUSIÓN

La innovación tecnológica no puede traducirse en vacío probatorio. Sin prueba técnicamente tratada, los derechos reconocidos en el mundo digital quedan sin tutela efectiva. Este proyecto no reemplaza al juez ni mecaniza la justicia: la refuerza, dotándola de instrumentos del siglo XXI con pleno respeto por el debido proceso.

Por ello, se solicita la sanción del presente proyecto de ley.

LIC. MARCELA MARINA PAGANO
DIPUTADA DE LA NACIÓN