

PROYECTO DE LEY DE DATOS PERSONALES

Análisis legal y comentarios



PROYECTO DE LEY DE DATOS PERSONALES

Análisis legal y comentarios

La presente publicación ha sido financiada por la Unión Europea. Su contenido es responsabilidad exclusiva de TEDIC y no refleja necesariamente los puntos de vista de la Unión Europea.



Financiado por
la Unión Europea

CON EL APOYO DE

La gente
cambia
el mundo

Diakonia

Tecnología
& Derechos
Humanos

TEDIC



Esta obra está disponible bajo licencia Creative

Commons Attribution 4.0 Internacional (CC BY SA 4.0)

<https://creativecommons.org/licenses/by-sa/4.0/deed.es>

TEDIC es una Organización No Gubernamental fundada en el año 2012, cuya misión es la defensa y promoción de los derechos humanos en el entorno digital. Entre sus principales temas de interés están la libertad de expresión, la privacidad, el acceso al conocimiento y género en Internet.

PROYECTO DE LEY DE DATOS PERSONALES

Análisis legal y comentarios

JULIO DE 2025

RESPONSABLE DEL ANÁLISIS LEGAL Y REDACCIÓN

Maricarmen Sequera Buzarquis

ASISTENCIA

Maricel Achucarro

COMUNICACIÓN

Romina Aquino González

DIAGRAMACIÓN

Horacio Oteiza

ACERCA DE LA AUTORA

Maricarmen Sequera Buzarquis: Abogada, Máster en Propiedad Intelectual por FLACSO Argentina. Especialista en Ciberseguridad por la Universidad de León y en Tecnopolítica por la Universidad de Barcelona. Fellow 2023 en el programa Global Competitiveness Leadership (GCL) Latin America and Caribbean Studies de la Universidad de Georgetown. Finalista de los Premios EQUALS in Tech 2021 y nombrada Heroína en los Premios RightsCon 2015 de Access Now. Miembro del Comité Regional de Subvenciones para América Latina y el Caribe de la Fundación Wikimedia – 2023-2025. Miembro de la red Global Future Councils del Foro Económico Mundial – 2025-2026.

1. TABLA DE CONTENIDO

PARECER LEGAL SOBRE LA LEY DE DATOS PERSONALES	5
1. ÁMBITO DE APLICACIÓN Y PRINCIPIO DE LEGALIDAD	6
2. PRINCIPIOS FUNDAMENTALES: CONSERVACIÓN Y RESPONSABILIDAD PROACTIVA	6
3. RELACIÓN CON EL DERECHO DE ACCESO A LA INFORMACIÓN PÚBLICA	7
4. TRANSFERENCIAS INTERNACIONALES DE DATOS	7
5. MANDATO DE LAS AUTORIDADES DE LA AGENCIA NACIONAL DE PROTECCIÓN DE DATOS PERSONALES	8
CONSIDERACIONES FINALES	8

PARECER LEGAL SOBRE LA LEY DE DATOS PERSONALES

Las organizaciones **TEDIC (Tecnología y Derechos Humanos¹)** y la **Coordinadora de Derechos Humanos del Paraguay (CODEHUPY)²**, comprometidas con la defensa y promoción de los derechos fundamentales en entornos digitales, realizan este análisis jurídico-técnico sobre el **proyecto de ley “Protección de Datos Personales” (Expediente D2162170)**, recientemente aprobado en la Cámara de Diputados y actualmente en etapa de revisión por la Cámara Alta.

Este parecer surge del seguimiento activo que las mismas realizan desde hace varios años al proceso legislativo en materia de privacidad, así como de la participación en la audiencia pública celebrada el 4 de julio de 2025, donde expusieron sus observaciones ante representantes del Congreso, de instituciones del Estado y de la sociedad civil.

Se reconoce el valor estratégico de este proyecto para establecer un marco normativo robusto y actualizado en materia de protección de datos personales en Paraguay y se celebra el avance institucional que representa haber alcanzado una versión sancionada por la Cámara de Diputados, tras un proceso deliberativo que incluyó más de una decena de sesiones, análisis artículo por artículo, y múltiples aportes desde diversos sectores.

Sin embargo, se considera que esta segunda etapa del procedimiento constitucional brinda una **oportunidad crucial para fortalecer la ley**, de forma que Paraguay no solo cuente con una norma adecuada, sino que se convierta en un referente regional en la defensa del derecho a la privacidad. En ese sentido, y con ánimo constructivo, se comparte a continuación las principales observaciones.

1 TEDIC: <https://www.tedic.org/>

2 CODEHUPY: <https://www.codehupy.org.py/>

2. ÁMBITO DE APLICACIÓN Y PRINCIPIO DE LEGALIDAD

El artículo 2 inciso b) excluye de manera general el tratamiento de datos personales realizados en contextos vinculados a la seguridad pública, defensa nacional, migración y procesos penales o de investigación criminal. Esta exclusión absoluta **deja sin resguardo normativo amplios sectores donde justamente se manejan datos sensibles**, y contradice los estándares internacionales que exigen que toda restricción al derecho a la privacidad sea justificada, necesaria y proporcional.

Se propone reemplazar esta cláusula por una **exclusión parcial** que limite ciertos derechos u obligaciones solo cuando sea imprescindible, sin eximir de forma total la aplicación de los principios básicos de protección de datos. Asimismo, es necesario especificar que dicha exclusión solo es válida cuando el tratamiento sea realizado por **autoridades públicas competentes**, evitando que entidades privadas puedan invocar indebidamente esta excepción.

3. PRINCIPIOS FUNDAMENTALES: CONSERVACIÓN Y RESPONSABILIDAD PROACTIVA

Si bien se celebra la inclusión de varios principios claves —como licitud, minimización, finalidad, transparencia y confidencialidad—, notamos la **ausencia expresa de dos principios esenciales**:

a. Conservación de datos personales

El tratamiento adecuado de datos personales debe incluir límites claros al **plazo de retención** de los mismos. Esta es una garantía elemental para proteger la privacidad y minimizar riesgos. Se propone incorporar un principio autónomo de conservación, que establezca que los datos solo podrán ser almacenados por el tiempo necesario para cumplir con su finalidad, debiendo ser eliminados una vez vencido ese plazo.

Países de la región ya cuentan con parámetros orientativos en esta materia, por ejemplo: 5 años para datos personales generales, entre 1 y 3 años para datos sensibles, y 30 días para videovigilancia. Estas referencias pueden ser útiles para establecer estándares nacionales y para que los responsables del tratamiento desarrollen políticas internas claras de eliminación segura.

b. Responsabilidad proactiva (accountability)

Este principio implica que las entidades responsables deben **demostrar activamente** que cumplen con la ley, mediante medidas organizacionales, políticas internas, formación continua del personal y registros documentados. Su inclusión explícita permite instalar una cultura institucional sólida de protección de datos y resulta especialmente relevante en contextos donde se utilice inteligencia artificial o sistemas automatizados.

Se considera que sustituir esta noción por la más general de “diligencia debida” diluye el alcance del principio. El concepto de **accountability**, recogido en instrumentos como el Reglamento General de Protección de Datos de la Unión Europea y el Convenio 108+, conlleva una **obligación verificable de cumplimiento y rendición de cuentas institucional**, especialmente exigible al sector público. Por tanto, recomendamos mantener esta denominación específica y su contenido conceptual completo.

4. RELACIÓN CON EL DERECHO DE ACCESO A LA INFORMACIÓN PÚBLICA

El artículo 24, tal como está redactado, introduce un procedimiento excesivamente complejo y ambiguo para el tratamiento de solicitudes de información pública que involucren datos personales. La posibilidad de que el titular de los datos deba ser notificado y dé su consentimiento puede entorpecer gravemente el ejercicio del derecho a la información, generando plazos indefinidos y una discrecionalidad peligrosa.

Es necesario **armonizar ambos derechos fundamentales —privacidad y acceso a la información—** aplicando principios reconocidos internacionalmente como el **test de daño**, el **test de interés público** y el **principio de divisibilidad**. Esto evitaría que la protección de datos se utilice como excusa para **ocultar información sobre el uso de recursos públicos, el desempeño de funcionarios o contrataciones estatales**, entre otros aspectos esenciales para la transparencia.

Se recomienda una redacción que respete el marco de la Ley N.º 5282/2014 y que limite las excepciones al acceso público solo cuando exista un riesgo real y demostrado a la privacidad, aplicando criterios proporcionales y objetivos.

5. TRANSFERENCIAS INTERNACIONALES DE DATOS

El artículo 19 establece una obligación general de adoptar “todas las acciones necesarias” en casos donde el país destinatario no cuente con nivel adecuado de protección. Consideramos importante **especificar cuáles son esas acciones**, incorporando ejemplos como cláusulas contractuales estándar, normas corporativas vinculantes, certificaciones o códigos de conducta.

También es fundamental definir que la **autoridad competente para evaluar la adecuación** de protección de un país extranjero será la Agencia Nacional de Protección de Datos Personales, quien podrá emitir resoluciones fundadas o listas oficiales para orientar a responsables y encargados.

6. MANDATO DE LAS AUTORIDADES DE LA AGENCIA NACIONAL DE PROTECCIÓN DE DATOS PERSONALES

El artículo 40 fija una duración de tres años para el mandato del Director General y su adjunto, con posibilidad de reelección. Consideramos que **este plazo es insuficiente** para asegurar estabilidad institucional, independencia política y continuidad en la implementación de políticas públicas de protección de datos.

Proponemos ampliar el mandato a **cinco (5) años**, limitando la reelección inmediata o autorizando una sola renovación, para favorecer la profesionalización del cargo, blindarlo frente a presiones externas y garantizar que las autoridades cuenten con el tiempo suficiente para desarrollar planes estratégicos sostenibles.

CONSIDERACIONES FINALES

Una ley de protección de datos personales moderna no puede limitarse a responder a urgencias coyunturales. Debe ser **una herramienta integral, anticipatoria, alineada con los derechos humanos** y capaz de adaptarse a las transformaciones tecnológicas en curso.

Desde TEDIC y CODEHUPY, se considera que los ajustes propuestos no solo son viables, sino necesarios para que esta legislación cumpla plenamente su objetivo: **garantizar de manera efectiva la protección del derecho a la privacidad, sin menoscabar otros derechos fundamentales como la transparencia, la libertad de expresión y el acceso a la información.**

