Asunción,11 de julio de 2025

A la Honorable Comisión de Ciencia y Tecnología
Cámara de Senadores del Congreso Nacional
Presente.

De nuestra mayor consideración:

Desde la Coalición de datos personales[1], facilitamos nuestro parecer técnico jurídico presentado en la audiencia pública del pasado 4 de julio de 2025.

El proyecto de ley "Protección de Datos Personales en Paraguay" expediente D2162170 fue presentado el 5 de mayo de 2021. Durante este periodo se llevaron a cabo 13 sesiones en las que se analizó el borrador de la ley. El 17 de diciembre de 2024, fue aprobada en general durante una sesión plenaria y remitida a comisiones para su análisis detallado, artículo por artículo. Durante los meses siguientes, las comisiones encargadas realizaron un exhaustivo estudio del proyecto e introdujeron diversas modificaciones. Finalmente, el 27 de mayo de 2025, fue aprobada en su totalidad, concluyendo así la primera etapa constitucional para la sanción de una ley.

Esta propuesta fue impulsada inicialmente en 2021 por la Comisión de Ciencia y Tecnología de la Cámara de Diputados y la Coalición de Datos Personales, conformada por organizaciones que, en algunos casos, llevan más de diez años abogando por una ley de este tipo en el país.

Con esta aprobación, el proyecto avanza a la segunda etapa del proceso constitucional, que consiste en su revisión por parte de la Cámara revisora. Para la Coalición de Datos Personales del Paraguay, este paso representa un avance significativo hacia la consolidación de un marco legal sólido en materia de privacidad. Aunque la versión original promovida por la Coalición incluía un enfoque más amplio, con un total de 85 artículos, el texto finalmente aprobado consta de 60 artículos, como resultado de las negociaciones y ajustes realizados durante el proceso legislativo.

Desafíos principales de la versión de Diputados

Fortalecer la ley a través de principios generales de datos personales claros y precisos.

Si bien se reconoce que varios de los artículos excluidos de la propuesta original presentada por la Coalición podrían ser abordados posteriormente en la etapa de

1Coalición de Datos personales: https://www.datospersonales.org.py/ (Integrada por APADIT, TEDIC, Puente y Internet Society)

reglamentación, hay aspectos clave que deberían ser afinados e incorporados nuevamente en forma expresa en la ley.

La propuesta legislativa actual incorpora principios generales fundamentales en materia de protección de datos personales, tales como la exactitud, licitud, minimización o proporcionalidad, lealtad y transparencia, finalidad, seguridad, confidencialidad y diligencia debida. No obstante, la ley no establece de forma explícita límites claros sobre la conservación de los datos personales ni contempla de manera expresa el principio de responsabilidad proactiva, ambos elementos esenciales para garantizar un marco normativo robusto y alineado con estándares internacionales.

a) Principio de legalidad. Este principio que se encuentra en el artículo 2, numeral 2, inciso b) del proyecto de ley, establece una exclusión total de su aplicación en relación con el tratamiento de datos personales efectuado con fines de seguridad pública, migración, defensa, seguridad nacional y en el marco de actividades penales, de investigación y represión del delito.

Consideramos que esta exclusión absoluta se aparta de estándares internacionales y debilita garantías institucionales y control ciudadano, al sustraer estas actividades del escrutinio y los principios básicos de protección de datos, sin sujetarlos a los principios mínimos, teniendo en cuenta, sobre todo, que se trata de ámbitos que incluyen datos sensibles.

Por ello, sugerimos se reemplace esta disposición por una exclusión parcial que permita limitar ciertos derechos u obligaciones en materia de protección de datos personales, solo en la medida en que sea estrictamente necesario y proporcional, debiendo observarse en todos los casos los principios generales de protección de datos personales, así como las garantías mínimas establecidas en la ley, en la medida que resulten compatibles.

Además, conforme a estándares internacionales, es fundamental determinar en el texto de la disposición que esta exclusión aplica únicamente al tratamiento efectuado por autoridades públicas competentes, limitando subjetivamente la excepción y no solamente en sentido material. De lo contrario, podría abrirse la posibilidad de que entidades privadas invoquen indebidamente esta excepción para sustraerse del cumplimiento de la ley y se sustraiga la exclusión a la vigencia del principio de competencia del derecho público.

Texto sugerido Artículo 2, numeral 2, inciso b):

> “b) Al tratamiento de datos personales efectuado por autoridades públicas competentes, en el ejercicio de sus atribuciones legales, con fines de prevención, investigación, detección, enjuiciamiento o sanción de infracciones penales, o para la protección y prevención frente a amenazas a la seguridad pública o la defensa nacional.

> Dicho tratamiento deberá respetar, en todo momento, los derechos y libertades fundamentales, aplicarse de manera necesaria y proporcionada al fin perseguido, y observar los principios generales de protección de datos personales, así como las garantías mínimas establecidas en la presente ley, en la medida que resulten compatibles con la naturaleza del tratamiento."

b) El principio de Conservación de datos personales. El principio de limitación del plazo de conservación establece que los datos personales no deben almacenarse por más tiempo del estrictamente necesario para cumplir con la finalidad para la cual fueron recolectados. Por ello, es fundamental que la ley defina plazos de retención apropiados y establezca mecanismos seguros para la eliminación de los datos una vez que hayan dejado de ser necesarios. A modo de referencia, en América Latina las tendencias en plazos de conservación varían según el tipo de datos: generalmente, datos personales se conservan por hasta 5 años, datos sensibles entre 1 y 3 años, documentación contable por un mínimo de 5 años, y registros de videovigilancia por alrededor de 1 mes. Estas prácticas pueden servir como guía para establecer estándares nacionales adecuados. (Internet Bolivia, 2025)

En este contexto, el Estado paraguayo debe avanzar en la definición de límites claros para los períodos de conservación de los datos personales, como parte esencial de una legislación robusta en materia de privacidad. Asimismo, los responsables de tratamiento de datos de terceros deben incorporar en sus políticas internas criterios precisos sobre los tiempos de retención y procedimientos de eliminación segura, especialmente en el tratamiento de datos sensibles.

Por ello, si bien el proyecto de ley hace referencia a la limitación del periodo de conservación dentro de lo establecido para el Principio de minimización o proporcionalidad, consideramos que el Principio de Conservación debe ser regulado en forma autónoma, conteniendo pautas claras relativas al plazo de conservación y no solamente relacionado al propósito o finalidad.

Texto sugerido:

> Artículo x. Limitación del plazo de conservación
>
> No podrán conservarse o mantenerse los datos durante más tiempo del necesario para los fines del tratamiento. La Autoridad de Control deberá establecer los plazos para la supresión y/o revisión periódica.
>
> El tratamiento ulterior de los datos personales con fines de archivo e interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales, siempre que se encuentren anonimizados o seudonimizados.

c) El principio de responsabilidad proactiva (accountability) implica que las organizaciones no solo deben cumplir con las normas de protección de datos personales, sino también demostrar activamente ese cumplimiento mediante políticas internas, procedimientos claros y evidencia documentada. Este enfoque transforma la privacidad en una obligación continua y transversal dentro de la gestión institucional. A diferencia del modelo tradicional, donde el cumplimiento era reactivo y se activaba ante incidentes o requerimientos regulatorios, la responsabilidad proactiva exige una actitud preventiva y sostenida. Esto incluye integrar la protección de datos en la estructura organizacional, aplicar medidas de seguridad, capacitar al personal y mantener registros de todas las acciones adoptadas para garantizar el cumplimiento. (Internet Bolivia, 2025)

Este principio, consagrado en normas como el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, marca un cambio cultural dentro de las organizaciones. La privacidad debe contemplarse desde el diseño de los procesos, incorporando evaluaciones de riesgo, medidas preventivas, asignación clara de responsabilidades y documentación sistemática, consolidando así una verdadera cultura de protección de datos desde adentro hacia afuera.

En el contexto del uso de inteligencia artificial para el tratamiento de datos personales, la aplicación del principio de responsabilidad proactiva será fundamental.

Si bien vemos que se referencia a ciertos componentes de este Principio dentro del artículo 4, inciso g) Principio de diligencia debida, consideramos que la sustitución del término "responsabilidad proactiva" por "diligencia debida", implica una alteración conceptual no menor. El principio de responsabilidad proactiva o “accountability”, recogido expresamente en el RGPD y en el Convenio 108+, incorpora una obligación activa de demostrar el cumplimiento de los principios de protección de datos ante la autoridad de control o los titulares, y constituye además una forma concreta de rendición de cuentas, especialmente exigible al sector público. En cambio, la diligencia debida remite a una noción más general de cumplimiento responsable, pero no necesariamente incluye el deber de demostrarlo ni la dimensión institucional de rendición de cuentas.

Por tanto, se sugiere mantener la denominación original del principio de responsabilidad proactiva (accountability), a fin de no debilitar los estándares internacionales en materia de cumplimiento verificable, transparencia y responsabilidad institucional y mantener el énfasis en la dimensión proactiva de la rendición de cuentas.

Texto sugerido:

> Sustituir el epígrafe del artículo 4, inciso g) “Principio de diligencia debida” por el de “Principio de responsabilidad proactiva”.

Fortalecer la ley a través de otros elementos esenciales del sistema

a) Acceso a la información pública. El artículo 24 de la ley sancionada en primera instancia del Congreso, introduce un procedimiento innecesariamente complejo para el acceso a la información pública, bajo el argumento de una posible “interferencia” con datos personales. Esta noción ambigua se presta a una interpretación discrecional y podría convertirse en una herramienta de uso arbitrario para denegar el acceso a información de interés público, debilitando así el derecho fundamental a la transparencia.

La Coalición de Datos Personales manifiesta su preocupación ante el contenido de este artículo. El procedimiento propuesto —que implica notificar al titular de los datos, esperar su consentimiento y eventualmente emitir un dictamen no vinculante — extiende de facto los plazos de respuesta mucho más allá del límite razonable previsto por la ley vigente Nº 5282/2014 Acceso a la Información Pública. Además, genera múltiples incertidumbres prácticas respecto a la notificación, su plazo y su ejecución. Esto no solo obstaculiza el ejercicio efectivo del derecho de acceso, sino que también permite que cualquier información vinculada a una persona en el Estado —sea funcionario o contratista— pueda quedar fuera del escrutinio público, incluso cuando se relacione directamente con el uso de fondos públicos.

Desde la Coalición de Datos recomendamos revisar y ajustar el Artículo 24 para evitar que se convierta en una barrera estructural al acceso a la información pública. Existen principios consolidados en los estándares internacionales, como el principio de divisibilidad, el test de daño y el test de interés público, que permiten armonizar adecuadamente la protección de datos personales con el derecho de la ciudadanía a la transparencia. Proteger la privacidad no debe utilizarse como excusa para opacar la rendición de cuentas y debilitar el control ciudadano sobre la gestión estatal.

La Ley de Acceso a la Información Pública y la protección de datos personales no son derechos en conflicto, sino dos caras de una misma moneda: se complementan y se equilibran mutuamente, sin anularse ni limitarse entre sí.

b) Transferencias internacionales. En relación a transferencias internacionales, en el segundo párrafo del artículo 19 se establece que, en caso de que el país destinatario no cuente con un nivel de protección adecuado, “el responsable o encargado debe efectuar todas las acciones necesarias para garantizar que el tratamiento de los datos personales se efectúe conforme a lo dispuesto en la presente ley.”

Se sugiere aclarar expresamente que dichas “acciones necesarias” incluyen la adopción de garantías adecuadas, tales como cláusulas contractuales específicas o estándares, normas corporativas vinculantes, códigos de conducta o mecanismos de certificación, conforme se detallan más adelante en el mismo artículo. Esta precisión contribuiría a dar más claridad al texto, dando el acento al concepto de

garantías, que reviste mayor relevancia e implicancia que el de “acciones”.

Por otra parte, el artículo no especifica quién ni cómo se determina si un país ofrece un nivel adecuado de protección de datos personales. Se sugiere incorporar expresamente que la evaluación de adecuación será realizada por la Agencia Nacional de Protección de Datos Personales, mediante resolución fundada, o a través de la publicación de una lista oficial de países o entidades que ofrecen garantías suficientes.

Por último, pero no menos importante, consideramos que el último párrafo del artículo debe ser suprimido, ya que contradice la lógica jurídica que justifica la enumeración de excepciones y entra en conflicto con el principio de legalidad.

El artículo establece de forma expresa los supuestos en los que los responsables o encargados del tratamiento quedan exceptuados del deber de garantizar que el tratamiento se realice conforme a la ley, conforme a estándares internacionales que definen esas situaciones con precisión, para evitar vacíos que pudieran comprometer los derechos tutelados.

Sin embargo, el párrafo final introduce la posibilidad de que la reglamentación amplíe dichas excepciones, lo cual resulta jurídicamente inadmisible. En materia de derechos fundamentales, las excepciones deben estar establecidas por ley en sentido estricto, no pudiendo ser ampliadas mediante norma reglamentaria. Habilitar tal posibilidad viola el principio de legalidad, que exige que toda excepción al deber de cumplimiento legal esté expresamente prevista en la norma legal y no sujeta a discrecionalidad reglamentaria.

Por lo tanto, en consideración a las razones expuestas, se propone la modificación del artículo en el siguiente sentido:

Texto sugerido:

> Artículo 19.- Reglas generales para las transferencias internacionales de datos personales.
>
> Las transferencias de datos personales fuera del territorio nacional, incluidas las transferencias ulteriores, sólo podrán realizarse si el país, territorio, sector u organización internacional destinataria ofrece un nivel de protección adecuado, conforme a lo dispuesto en la presente ley.
>
> La evaluación de la adecuación será realizada por la Agencia Nacional de Protección de Datos Personales, y determinada mediante resolución fundada o a través de la publicación de una lista oficial, de conformidad con los principios, derechos y garantías establecidos en esta ley.
>
> En caso de que el país destinatario no cuente con un nivel de protección adecuado, el responsable o encargado debe adoptar garantías

apropiadas para asegurar que el tratamiento de los datos personales se efectúe conforme a lo dispuesto en la presente ley, que podrán consistir, entre otras, en cláusulas contractuales específicas o estándares, normas corporativas vinculantes, códigos de conducta o mecanismos de certificación, conforme se detallan en el presente artículo.

No se aplica lo dispuesto en el párrafo anterior, en los siguientes casos:

1. Acuerdos en el marco de tratados internacionales en los cuales la República del Paraguay sea parte;

2. Cooperación judicial internacional;

3. Cooperación internacional entre organismos de inteligencia para la lucha contra el terrorismo, tráfico ilícito de drogas, lavado de activos, corrupción, trata de personas y otras formas de criminalidad organizada;

4. Cuando los datos personales sean necesarios para la ejecución de una relación contractual en la que el titular de datos personales sea parte, incluyendo lo necesario para actividades como la autentificación de usuario, mejora y soporte del servicio, monitoreo de la calidad del servicio, soporte para el mantenimiento y facturación de la cuenta y aquellas actividades que el manejo de la relación contractual requiera;

5. Cuando se trate de transferencias bancarias o bursátiles, en lo relativo a las transacciones respectivas y conforme a la ley aplicable;

6. Cuando el flujo transfronterizo de datos personales se realice para la protección, prevención, diagnóstico o tratamiento médico o quirúrgico de su titular; o cuando sea necesario para la realización de estudios epidemiológicos o análogos, en tanto se apliquen procedimientos de anonimización adecuados;

7. Cuando el titular de los datos personales haya dado su consentimiento previo, informado, expreso e inequívoco;

8. Cuando el responsable del tratamiento ofrezca y acredite garantías de cumplimiento de los principios, los derechos del interesado y el régimen de protección de datos previsto en esta ley, en forma de:

    a) Cláusulas contractuales específicas para una determinada transferencia;

    b) Cláusulas contractuales estándares;

c) Normas corporativas globales;

d) Sellos, certificados y códigos de conducta emitidos periódicamente.

c) Director de la Agencia Nacional de Protección de Datos Personales. El artículo 40 establece que el Director General y su adjunto permanecerán en el cargo por un período de tres años, con posibilidad de reelección. Si bien la posibilidad de renovación introduce cierta flexibilidad, consideramos que el plazo inicial resulta breve ya que se busca garantizar independencia, estabilidad institucional y continuidad en la implementación de políticas públicas. Proponemos extender el mandato inicial a cinco (5) años sin posibilidad de reelección inmediata o con una única reelección.

Texto sugerido:

Artículo 40.- Duración del cargo y remoción.

El Director General de la Agencia Nacional de Protección de Datos Personales y el adjunto durarán 5 (cinco) años en el cargo, pudiendo ser designados nuevamente para periodos posteriores.

d) Oficial de Protección de datos personales: La propuesta original, en línea con las buenas prácticas en la materia, determinaba aquellos supuestos en los que resulta obligatoria la designación de un oficial de protección de datos, en atención al tratamiento que se realice, ya se porque se trate de una autoridad u organismo público, por la escala o volúmen de datos que se traten, especialmente si son datos sensibles, así como si el tratamiento constituye la actividad principal del responsable.

Esta determinación de los supuestos en los que resulta obligatoria la designación de un oficial, en la actual versión ha sido relegada a la reglamentación, al igual que las funciones mínimas que corresponden al mismo. La obligatoriedad de designar un oficial para ciertos sujetos, con la carga y responsabilidad que ello implica, estimamos que es un aspecto que debe ser establecido en el cuerpo de la ley, a fin de asegurar su fuerza normativa y evitar que quede sujeto a modificaciones o relativizaciones mediante disposiciones reglamentarias de menor jerarquía.

Además, la designación de un oficial forma parte del Principio de responsabilidad proactiva y debe ser promovida en la mayor parte de sectores, más allá de aquellos que la ley ya establece como mínimos y obligatorios. Por ello, se sugiere reincorporar en el artículo respectivo de la ley, aquellos supuestos en los que resulta obligatoria la designación de un oficial de protección de datos personales.

Texto sugerido:

“Artículo 18.- Oficial de protección de datos.

Los responsables y encargados del tratamiento deberán designar un oficial de protección de datos en cualquiera de los siguientes supuestos:

1. Cuando revistan el carácter de autoridades u organismos públicos; excepto el Poder Judicial en tanto se encuentre en ejercicio de su función judicial;

2. Se realice tratamiento a gran escala de datos sensibles o de datos personales relativos a condenas e infracciones penales como parte de la actividad principal del responsable o encargado del tratamiento;

3. Las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de los titulares de datos a gran escala.

El oficial de protección de datos será designado atendiendo a sus cualidades profesionales y a su capacidad para desempeñar las funciones a ser establecidas en la reglamentación de la presente ley.Texto sugerido:

“Artículo 18.- Oficial de protección de datos.

Los responsables y encargados del tratamiento deberán designar un oficial de protección de datos en cualquiera de los siguientes supuestos:

4. Cuando revistan el carácter de autoridades u organismos públicos; excepto el Poder Judicial en tanto se encuentre en ejercicio de su función judicial;

5. Se realice tratamiento a gran escala de datos sensibles o de datos personales relativos a condenas e infracciones penales como parte de la actividad principal del responsable o encargado del tratamiento;

6. Las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de los titulares de datos a gran escala.

El oficial de protección de datos será designado atendiendo a sus cualidades profesionales y a su capacidad para desempeñar las funciones a ser establecidas en la reglamentación de la presente ley.

Un grupo empresarial podrá nombrar un único oficial de protección de datos siempre que sea fácilmente accesible desde cada establecimiento.

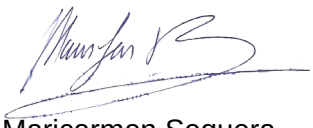
Cuando el responsable o el encargado del tratamiento sea una autoridad

> u organismo público, se podrá designar un único oficial de protección de datos para varias de estas autoridades u organismos, teniendo en cuenta su estructura organizativa y tamaño.
>
> El oficial de protección de datos podrá formar parte del personal del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios.
>
> La reglamentación establecerá otros aspectos relativos al oficial de protección de datos".

Cada uno de los aspectos señalados, responde a la necesidad inaplazable de contar con una ley de protección de datos personales sólida, integral y actualizada. Esta normativa debe anticiparse a los desafíos tecnológicos emergentes, y no limitarse a soluciones parciales o apresuradas que acaban requiriendo enmiendas constantes por falta de previsión adecuada. Solo con un marco legal robusto será posible garantizar una protección efectiva de los derechos fundamentales en la era digital.

Consideramos que este aporte técnico específico representa una contribución valiosa para el fortalecimiento de la ley en su aplicación práctica en Paraguay. Confiamos que las comisiones técnicas del Senado del Congreso Nacional sabrán valorar su importancia.

Atentamente,



Maricarmen Sequera
TEDIC

Giuliana Galli
Puente

Natalia Enciso
APADIT

Cecilia Abente
APADIT

Referencias bibliográficas:

1) Internet Bolivia (2025). Guia de Implementación de Protección de Datos y Uso Responsable de Inteligencia Artificial en Bolivia. En https://internetbolivia.org/wp-content/uploads/2025/05/guia_proteccion_datos_web.pdf
2) Federico Legal (2025) Opinión preliminar del experto en Acceso a la información pública. En https://x.com/federicolegal/status/1943048423302672822?s=48