Revista UNIDA Científica
e-ISSN: 2520-9213

Publicación periódica de acceso abierto, financiada y editada por la Universidad de la Integración de las Américas

https://doi.org/10.69940/ruc.20261207

Artículo original

Protección de datos personales en Paraguay y Chile: análisis comparado y evaluación frente al estándar del GDPR

Data Protection in Paraguay and Chile: A Comparative Analysis and Assessment Against the GDPR Standard

Tamara Tischler W[1]

[1] Ceres Group S.A., Asunción, Paraguay.

RESUMEN

El artículo presenta un análisis comparado de la Ley N.º 7593/2025, De Protección de Datos Personales en la República del Paraguay; su antecedente, la Ley N.º 6534/2020, De Protección de Datos Personales Crediticios; las leyes chilenas N.º 21.719 y N.º 21.663; y el Reglamento General de Protección de Datos (General Data Protection Regulation [GDPR]) de la Unión Europea. El objetivo es evaluar el grado de adecuación normativa e institucional de Paraguay al estándar internacional, considerando las deficiencias evidenciadas durante la crisis de ciberseguridad de 2025. Se emplea un enfoque cualitativo, un diseño no experimental y un alcance descriptivo-analítico, mediante una metodología jurídico-comparada de carácter estructural y el análisis documental de normas, doctrina especializada e informes institucionales. La comparación se organiza según principios rectores, derechos de los titulares, responsabilidad proactiva, brechas de seguridad, transferencias internacionales, tratamiento automatizado, autoridades de control y sanciones. Los resultados muestran que la nueva legislación paraguaya aproxima formalmente el país al GDPR y supera el modelo sectorial anterior. Sin embargo, persisten desafíos relacionados con la implementación de la autoridad de control, la coordinación institucional y las capacidades técnicas para prevenir y responder a incidentes. El modelo chileno presenta una mayor especialización al diferenciar la supervisión jurídica de la gestión técnica de la ciberseguridad. Se concluye que la eficacia del régimen paraguayo dependerá de la autonomía y los recursos de la autoridad, la aplicación de la responsabilidad proactiva y la articulación con los organismos de ciberseguridad para transformar las garantías normativas en una protección efectiva de los derechos fundamentales.

Palabras clave: Chile; Derecho comparado; GDPR; Paraguay; Protección de datos personales.

ABSTRACT

This article presents a comparative analysis of Paraguay's Law No. 7593/2025, Law on the Protection of Personal Data in the Republic of Paraguay; its predecessor, Law No. 6534/2020, Law on the Protection of Personal Credit Data; Chile's Laws No. 21,719 and No. 21,663; and the European Union's General Data Protection Regulation (GDPR). The objective is to assess Paraguay's degree of normative and institutional alignment with the international standard, considering the shortcomings revealed during the 2025 cybersecurity crisis. The study uses a qualitative approach, a non-experimental design, and a descriptive-analytical scope, through a structural comparative legal methodology and the documentary analysis of legislation, specialized scholarship, and institutional reports. The comparison is organized according to governing principles, data subject rights, accountability, data breaches, international transfers, automated processing, supervisory authorities, and sanctions. The results show that Paraguay's new legislation formally brings the country closer to the GDPR and overcomes the previous sectoral model. However, challenges persist regarding the implementation of the supervisory authority, institutional coordination, and technical capabilities to prevent and respond to incidents. The Chilean model presents greater specialization by distinguishing legal supervision from the technical management of cybersecurity. It is concluded that the effectiveness of Paraguay's regime will depend on the authority's autonomy and resources, the application of accountability, and coordination with cybersecurity agencies to transform normative guarantees into effective protection of fundamental rights.

Keywords: Chile; Comparative law; Data protection; GDPR; Paraguay.

INTRODUCCIÓN

El presente artículo tiene como objetivo evaluar el grado de adecuación del nuevo régimen paraguayo de protección de datos personales al estándar internacional establecido por el Reglamento General de Protección de Datos de la Unión Europea (GDPR), considerando las deficiencias institucionales evidenciadas durante la crisis sistémica de ciberseguridad de 2025, caracterizada por ataques coordinados contra múltiples instituciones públicas, interrupciones de servicios y vulneraciones de datos (Ministerio de Tecnologías de la Información y Comunicación [MITIC], 2025a, 2025b).

Para ello, se compara la evolución normativa de Paraguay con el modelo chileno, seleccionado por constituir uno de los referentes latinoamericanos de mayor actualidad, especialización institucional y convergencia con el estándar europeo.

La protección de los datos personales constituye un componente central de los debates contemporáneos sobre derechos fundamentales, soberanía tecnológica y gobernanza digital.

Para correspondencia dirigirse a: tamaratischlerw@gmail.com
Recibido: 05 de febrero de 2026. **Aceptado:** 20 de julio de 2026
Conflictos de interes: Ninguna que declarar. **Fuente de financiamiento:** Ninguno. **Editor responsable:** Nadia Glavinich

Este es un artículo publicado en Acceso Abierto bajo Licencia Creative Commons CC-BY, que permite el uso sin restricciones, distribución y reproducción en cualquier medio, siempre que se cite debidamente la obra original.

En un entorno caracterizado por el tratamiento masivo de información, la opacidad y las asimetrías informativas generan riesgos para la privacidad, la dignidad y la autodeterminación informativa. Por ello, los marcos regulatorios deben garantizar derechos exigibles, fortalecer la confianza institucional y ofrecer seguridad jurídica para los flujos transfronterizos de datos.

El GDPR se ha consolidado como el principal paradigma internacional en esta materia, mediante un modelo basado en principios, responsabilidad proactiva y autoridades de control independientes. Su influencia ha impulsado reformas en América Latina, aunque con distintos niveles de madurez normativa e institucional. Paraguay, que hasta 2025 contaba únicamente con una regulación sectorial vinculada con los datos crediticios, promulgó la Ley N.º 7593/2025 como su primer régimen integral de protección de datos personales.

La Ley N.º 7593/2025 fue promulgada y publicada el 27 de noviembre de 2025, pero entrará en vigor una vez transcurridos veinticuatro meses desde su publicación oficial, conforme con su artículo 57. Por consiguiente, el período actual corresponde a una etapa de transición y preparación institucional previa a su plena implementación.

Chile ofrece un contraste especialmente pertinente porque combina la Ley N.º 21.719, que reforma el régimen de protección y tratamiento de datos personales y crea una autoridad especializada, con la Ley Marco de Ciberseguridad N.º 21.663 y la Agencia Nacional de Ciberseguridad (Ley N.º 21.663, 2024; Ley N.º 21.719, 2024). Esta arquitectura permite examinar un modelo que diferencia la supervisión jurídica del tratamiento de datos de la prevención y respuesta técnica frente a incidentes, ofreciendo elementos útiles para evaluar los desafíos de implementación del sistema paraguayo.

La comparación se orienta a identificar convergencias, brechas y desafíos relacionados con los principios rectores, los derechos de los titulares, la responsabilidad proactiva, la gestión de brechas y la autonomía de las autoridades de control. El estudio también resulta relevante para el Mercado Común del Sur (MERCOSUR), donde la creciente digitalización exige marcos compatibles que permitan la circulación transfronteriza de datos personales bajo garantías adecuadas de protección. Asimismo, se vincula con la práctica profesional de la autora en consultoría jurídica sobre ciberseguridad, protección de datos y cumplimiento normativo.

MATERIALES Y MÉTODOS

El estudio adopta un enfoque cualitativo, un diseño no experimental y un alcance descriptivo-analítico. Se emplea una metodología jurídico-comparada de carácter estructural, sustentada en el análisis documental de legislación, doctrina especializada, informes institucionales e instrumentos internacionales. El Reglamento General de Protección de Datos de la Unión Europea (GDPR) se utiliza como parámetro común para examinar instituciones jurídicas equivalentes e identificar convergencias, divergencias y distintos niveles de adecuación normativa e institucional entre Paraguay y Chile.

El análisis se desarrolló en tres etapas. En la primera, se identificaron y seleccionaron las fuentes normativas, doctrinales e institucionales relacionadas directamente con la protección de datos personales, la ciberseguridad y la actuación de las autoridades de control. En la segunda, las fuentes fueron clasificadas conforme con las categorías previamente definidas: principios rectores, derechos de los titulares, bases de licitud, responsabilidad proactiva, gestión de brechas de seguridad, transferencias internacionales, tratamiento automatizado, autoridad de control y régimen sancionatorio. En la tercera etapa, se realizó un contraste sistemático entre los marcos jurídicos de Paraguay y Chile, utilizando el GDPR como parámetro de referencia para determinar sus principales coincidencias, diferencias y desafíos de implementación.

La delimitación espacial comprende los ordenamientos jurídicos de Paraguay y Chile, mientras que el GDPR se incorpora como estándar internacional de comparación y no como un tercer caso nacional. En términos temporales, el corpus examinado reúne fuentes publicadas entre 1980 y 2025, período que comprende desde la Constitución Política de la República de Chile hasta la promulgación de la Ley paraguaya N.º 7593/2025 y los informes institucionales sobre la crisis de ciberseguridad ocurrida durante ese año.

Las fuentes fueron seleccionadas conforme con criterios de pertinencia temática, actualidad normativa, autoridad institucional y utilidad para las categorías de comparación. Se incluyeron normas que regulan directamente la protección de datos personales y la ciberseguridad, doctrina especializada sobre el GDPR e informes institucionales relacionados con los incidentes analizados. Se excluyeron otros ordenamientos latinoamericanos debido al carácter focalizado del estudio, así como documentos que no presentaban una relación directa con el objeto o las categorías de análisis.

RESULTADOS

El GDPR como parámetro normativo

El GDPR constituye el principal parámetro internacional de referencia en materia de protección de datos personales. Su modelo se estructura sobre principios de licitud, transparencia, limitación de la finalidad, minimización, exactitud, seguridad y responsabilidad proactiva, acompañados de derechos exigibles para los titulares (Kuner et al., 2020; Reglamento Unión Europea 2016/679).

El GDPR exige que responsables y encargados adopten medidas técnicas y organizativas proporcionales al riesgo y puedan demostrar el cumplimiento normativo. Para ello, incorpora mecanismos como la protección de datos desde el diseño y por defecto, los registros de actividades, las evaluaciones de impacto, la notificación de brechas y la supervisión ejercida por autoridades independientes. Su alcance extraterritorial y su influencia sobre las reformas latinoamericanas justifican su utilización como parámetro común de comparación (Greenleaf, 2023; Reglamento Unión Europea 2016/679, art. 3).

Evolución normativa de Paraguay

Del modelo sectorial al régimen integral de protección de datos

Hasta la promulgación de la Ley N.º 7593/2025, Paraguay carecía de un régimen general de protección de datos personales. La Ley N.º 6534/2020 regulaba principalmente el tratamiento de información crediticia y respondía a una lógica sectorial vinculada con la protección del consumidor financiero.

Este modelo no establecía un sistema transversal aplicable a los sectores público y privado, ni reconocía integralmente principios, derechos, obligaciones de seguridad y mecanismos institucionales de supervisión. En consecuencia, numerosos tratamientos vinculados con la salud, la educación, los servicios digitales y la Administración Pública permanecían fuera de un marco general de protección de datos, debido al alcance sectorial de la normativa vigente (Ley N.º 6534/2020).

La Ley N.º 7593/2025 y la configuración del régimen integral

La Ley N.º 7593/2025 configura el primer régimen general de protección de datos personales de Paraguay, aplicable a los sectores público y privado, aunque su entrada en vigor se encuentra diferida hasta el 27 de noviembre de 2027. La norma reconoce principios de tratamiento, derechos de los titulares, bases de licitud, deberes de seguridad, obligaciones de notificación de brechas, reglas para las transferencias

internacionales y garantías frente a determinadas decisiones automatizadas.

Asimismo, prevé una autoridad especializada de protección de datos y un régimen administrativo de supervisión y sanción. De esta manera, el ordenamiento paraguayo transita desde una regulación limitada a la información crediticia hacia un sistema transversal de tutela de los datos personales.

Configuración normativa e institucional de Chile

Evolución del marco jurídico: de la Ley N.º 19.628 a la Ley N.º 21.719

La Ley N.º 19.628 (1999), pionera en la región desde 1999, resultó insuficiente frente al tratamiento masivo de datos al carecer de una autoridad especializada y de garantías como la portabilidad y la responsabilidad proactiva. La Ley N.º 21.719 (2024), cuya entrada en vigor está prevista para el 1 de diciembre de 2026, reforma estructuralmente este régimen e incorpora un modelo basado en la autodeterminación informativa, la gestión del riesgo y la capacidad de demostrar el cumplimiento, aproximando el ordenamiento chileno al paradigma del GDPR.

El nuevo marco fortalece los principios y derechos aplicables al tratamiento, crea la Agencia de Protección de Datos Personales y establece potestades de supervisión y sanción. Esta transformación se complementa con el reconocimiento constitucional de la protección de los datos personales en el artículo 19 N.º 4, configurando una tutela jurídica e institucional más robusta que la prevista por el régimen anterior (Constitución Política de la República de Chile, 1980, art. 19 N.º 4).

La Ley Marco de Ciberseguridad N.º 21.663 y la especialización institucional

La Ley N.º 21.663 (2024) creó la Agencia Nacional de Ciberseguridad (ANCI) y estableció obligaciones de prevención, gestión de riesgos y reporte de incidentes aplicables, entre otros, a los prestadores de servicios esenciales y Operadores de Importancia Vital.

El ordenamiento chileno diferencia las funciones de protección de datos personales de las competencias relativas a la ciberseguridad. Conforme al nuevo diseño institucional, la Agencia de Protección de Datos Personales supervisará jurídicamente el tratamiento y tutelará los derechos de los titulares, mientras que la ANCI coordina la prevención y respuesta frente a incidentes. Esta distribución configura un sistema institucional especializado y articulado entre supervisión jurídica y gestión técnica de la seguridad de la información.

Comparación normativa entre Paraguay, Chile y el GDPR

La Tabla 1 presenta los resultados de la comparación entre la Ley paraguaya N.º 7593/2025, las leyes chilenas N.º 21.719 y N.º 21.663 y el GDPR, conforme con las categorías de análisis definidas en la metodología.

La crisis de ciberseguridad de 2025 como resultado del análisis documental

El año 2025 representó una crisis sistémica para el modelo de confianza digital en Paraguay, al comprometer la tríada de la seguridad de la información: confidencialidad, integridad y disponibilidad. Durante el primer semestre, grupos como CyberTeam, Leaker y Brigada Cyber PMC se atribuyeron públicamente ataques contra organismos estatales. El Ministerio de Tecnologías de la Información y Comunicación [MITIC] (2025b) confirmó dieciocho incidentes, incluyendo casos de *defacement*, captura de información y accesos no autorizados que afectaron a ministerios y otras instituciones públicas.

Paralelamente, se reportaron prácticas de extorsión basadas en datos robados y el posible uso de *infostealers*, vinculadas con conjuntos que comprendían entre 5,5 y 7,4 millones de registros ciudadanos, incluidos nombres, cédulas, domicilios e información relacionada con registros de salud. No obstante, los análisis disponibles indican que una parte de los archivos correspondía a filtraciones anteriores, mientras que otros contenían registros y marcas temporales de 2025, por lo que no puede atribuirse la totalidad de la información a un único

Tabla 1. Comparación normativa

Eje	Paraguay	Chile	GDPR
Alcance	Régimen general para los sectores público y privado.	Régimen general complementado por la legislación de ciberseguridad.	Régimen general con alcance extraterritorial.
Principios y licitud	Licitud, finalidad, proporcionalidad, calidad, transparencia y seguridad.	Licitud, finalidad, proporcionalidad, transparencia y responsabilidad.	Licitud, lealtad, transparencia, minimización y responsabilidad proactiva.
Derechos	Acceso, rectificación, supresión, oposición, portabilidad y garantías frente a decisiones automatizadas.	Acceso, rectificación, supresión, oposición, portabilidad y protección frente al tratamiento automatizado.	Acceso, rectificación, supresión, oposición, limitación, portabilidad y garantías frente a decisiones automatizadas.
Responsabilidad proactiva	Medidas técnicas y organizativas y deberes de seguridad.	Gestión del riesgo, medidas preventivas y deberes de cumplimiento.	Privacidad desde el diseño, registros y evaluaciones de impacto.
Brechas de seguridad	Notificación a la autoridad y, según el riesgo, a los titulares.	Reporte y gestión de incidentes con intervención de la ANCI.	Notificación a la autoridad, por regla general, dentro de las 72 horas.
Transferencias	Adecuación y garantías suficientes.	Condiciones de protección y mecanismos de transferencia.	Adecuación, cláusulas contractuales y otras garantías.
Institucionalidad	Autoridad especializada en proceso de implementación.	Agencia de Protección de Datos Personales y Agencia Nacional de Ciberseguridad (ANCI).	Autoridades de control independientes.
Sanciones	Multas graduadas según la gravedad.	Sanciones administrativas según categorías y agravantes.	Hasta EUR 20 millones o el 4 % de la facturación global anual.

Fuente. Elaboración propia con base en la Ley N.º 7593/2025, la Ley N.º 21.719 (2024), la Ley N.º 21.663 (2024) y el Reglamento Unión Europea 2016/679.

incidente (Resecurity, 2025).

Los análisis de inteligencia de amenazas posteriores sugirieron que uno de los posibles vectores de acceso fue el compromiso de terminales utilizadas por funcionarios o personal vinculado con sistemas gubernamentales. El *malware* de robo de información habría permitido obtener credenciales válidas y acceder a determinados portales como usuarios autenticados, sin necesidad de explotar vulnerabilidades de día cero complejas. Estos indicios permiten inferir debilidades en la protección de los dispositivos finales, la gestión de identidades, el principio de mínimo privilegio y la autenticación multifactor, aunque la evidencia pública disponible no permite reconstruir de manera concluyente las fases de movimiento lateral o escalamiento de privilegios para todos los incidentes (MITIC, 2025b; Resecurity, 2025).

La reacción estatal ante este escenario fue predominantemente reactiva y estuvo acompañada de información pública limitada sobre el origen, alcance y actualidad de los datos comprometidos. El MITIC, a través del CERT-PY, informó haber activado procedimientos de contención, análisis y restablecimiento de los sistemas; sin embargo, las discrepancias existentes respecto de la magnitud de la filtración dificultaron que la ciudadanía pudiera conocer con precisión los riesgos derivados de la exposición. La comunicación institucional no proporcionó inicialmente información homogénea sobre los datos afectados ni sobre las medidas personales de mitigación, como el cambio de contraseñas, el monitoreo de accesos y la prevención del fraude de identidad (MITIC, 2025a, 2025b; Resecurity, 2025).

DISCUSIÓN

Alcance de la adecuación normativa paraguaya

Los resultados muestran que la Ley N.º 7593/2025 aproxima formalmente a Paraguay al estándar del GDPR mediante la adopción de un régimen general, el reconocimiento de derechos, la incorporación de obligaciones de seguridad y la previsión de una autoridad especializada. Este avance supera la fragmentación del modelo limitado a los datos crediticios y fortalece la tutela de la autodeterminación informativa.

Sin embargo, la convergencia normativa no equivale automáticamente a una protección efectiva. La adecuación material dependerá de la reglamentación de la ley, de la capacidad de fiscalización y sanción y de la implementación de mecanismos que permitan demostrar el cumplimiento y gestionar los riesgos asociados al tratamiento de datos personales.

La crisis de ciberseguridad de 2025 y las debilidades de gobernanza

La doctrina especializada sostiene que los incidentes masivos de ciberseguridad que comprometen datos personales no constituyen únicamente fallas tecnológicas, sino también fallas de gobernanza digital y de protección efectiva de derechos fundamentales, en la medida en que evidencian deficiencias institucionales en la gestión del riesgo, la supervisión y la rendición de cuentas (European Union Agency for Cybersecurity, 2024).

La posterior publicación de los conjuntos de datos en foros clandestinos evidenció la necesidad de fortalecer arquitecturas basadas en *Zero Trust* (Confianza Cero), mecanismos de *Data Loss Prevention* (DLP), segmentación de redes y cifrado de datos en reposo mediante estándares criptográficos robustos. Sin embargo, estos controles deben presentarse como medidas técnicas necesarias a partir de los riesgos observados, puesto que no se dispone de una auditoría pública que confirme su ausencia generalizada en todas las instituciones afectadas. La exposición de archivos y bases de datos demuestra, en cualquier caso, que la utilización de credenciales válidas puede neutralizar los controles perimetrales cuando no existen mecanismos suficientes de verificación continua, monitoreo de sesiones y detección de comportamientos anómalos.

Esta respuesta evidenció la necesidad de contar con un Sistema de Gestión de Seguridad de la Información (SGSI) integrado y con una autoridad especializada capaz de supervisar la actuación de los responsables del tratamiento. Asimismo, puso de manifiesto la importancia de establecer protocolos obligatorios de notificación de brechas que permitan informar oportunamente a los titulares sobre la naturaleza de los datos comprometidos, las consecuencias previsibles y las medidas adoptadas para reducir los riesgos.

La exigencia de USD 7,4 millones y la posterior difusión de los archivos evidenciaron la presión ejercida por los grupos de cibercrimen organizado sobre la capacidad estatal de respuesta y recuperación. Aunque las fuentes públicas no permiten afirmar que los servicios críticos permanecieran indisponibles durante semanas ni que existiera una falla generalizada de los planes de recuperación ante desastres (DRP), los incidentes demostraron la necesidad de fortalecer la continuidad operativa, el respaldo de la información y los procedimientos de restauración segura (Resecurity, 2025).

Este escenario de fragilidad sistémica reforzó la urgencia política y operativa de contar con un régimen integral de protección de datos personales. No obstante, la Ley N.º 7593/2025 no surgió exclusivamente como consecuencia de los incidentes, debido a que su proceso de elaboración e incidencia legislativa se había iniciado varios años antes. La crisis de 2025 confirmó, más bien, la relevancia práctica de la reforma y la necesidad de integrar la ciberseguridad, el *hardening* de sistemas y la privacidad desde el diseño como requisitos esenciales para la protección de la soberanía informativa y los derechos fundamentales de la ciudadanía paraguaya (Ley N.º 7593/2025; TEDIC, 2025).

Desde la perspectiva jurídica, la crisis demostró que la ausencia de un régimen integral de protección de datos personales no solo dificultaba la tutela efectiva de los derechos de los ciudadanos, sino que también impedía exigir responsabilidades claras a los organismos encargados del tratamiento de la información. La inexistencia de obligaciones generales en materia de seguridad, notificación de brechas y supervisión institucional evidenció las limitaciones del modelo normativo vigente hasta ese momento.

Limitaciones institucionales y desafíos de implementación de la Ley N.º 7593/2025

La crisis de 2025 evidenció que las deficiencias del modelo paraguayo no eran exclusivamente tecnológicas, sino también institucionales. Antes de la Ley N.º 7593/2025, el MITIC y el CERT-PY ejercían funciones relacionadas con la prevención y respuesta técnica ante incidentes, pero no contaban con las competencias jurídicas, la autonomía ni las potestades sancionatorias propias de una autoridad de protección de datos.

La dependencia orgánica del MITIC respecto del Poder Ejecutivo podía generar tensiones frente a tratamientos realizados por la propia Administración Pública. Además, sus funciones no comprendían integralmente la tutela de los derechos de acceso, rectificación, supresión, oposición y portabilidad, ni la fiscalización general del cumplimiento de las obligaciones relativas al tratamiento de datos personales.

La implementación de la Ley N.º 7593/2025 requiere, por tanto, una autoridad especializada con autonomía funcional, capacidad técnica, presupuesto suficiente y facultades efectivas de supervisión y sanción. Sin estas condiciones, existe el riesgo de que las garantías reconocidas normativamente no se traduzcan en mecanismos efectivos de protección.

Diferencias de madurez institucional entre Paraguay, Chile y el GDPR

La comparación revela una convergencia progresiva de los

tres ordenamientos en materia de derechos, responsabilidad proactiva y gestión de brechas. Paraguay y Chile incorporan elementos del modelo europeo, aunque presentan diferentes niveles de desarrollo institucional y capacidad operativa.

El modelo chileno evidencia una mayor especialización al distribuir las competencias entre la Agencia de Protección de Datos Personales y la ANCI. Esta separación permite distinguir la supervisión jurídica del tratamiento de datos de la prevención y respuesta técnica frente a incidentes. Paraguay, en cambio, se encuentra en una etapa de transición y preparación institucional previa a la entrada en vigor de la Ley N.º 7593/2025, por lo que la eficacia de su nuevo régimen dependerá de la consolidación de la autoridad de control y de su coordinación con los organismos responsables de la ciberseguridad.

En este contexto, la principal brecha paraguaya no reside actualmente en la ausencia de una ley general, sino en la capacidad institucional para aplicar el principio de responsabilidad proactiva, fiscalizar el cumplimiento y responder eficazmente frente a incidentes que comprometan datos personales. La experiencia chilena muestra que la tutela efectiva requiere articular regulación jurídica, gestión del riesgo y capacidades técnicas especializadas.

Los resultados muestran que la aproximación normativa de Paraguay y Chile al GDPR se inscribe en la expansión internacional de las legislaciones de protección de datos documentada por Greenleaf (2023). El modelo utilizado como parámetro de comparación corresponde al marco regulatorio analizado por Kuner et al. (2020), que presenta al GDPR como una transformación sustancial del sistema europeo de protección de datos. Sin embargo, los hallazgos del caso paraguayo indican que la convergencia normativa no garantiza por sí sola una protección efectiva. La información publicada por el MITIC (2025a, 2025b) y Resecurity (2025) evidencia que la eficacia del régimen también depende de la capacidad institucional para prevenir incidentes, verificar su alcance, responder técnicamente y comunicar oportunamente los riesgos. En consecuencia, el estudio permite identificar una distancia entre la adopción formal del estándar internacional y las capacidades necesarias para su implementación efectiva.

Fortalezas, limitaciones y líneas futuras

La principal fortaleza de la metodología jurídico-comparada empleada consiste en utilizar el GDPR como parámetro común para examinar ordenamientos con diferentes niveles de desarrollo normativo e institucional. La definición previa de categorías de análisis permitió organizar sistemáticamente la comparación entre Paraguay y Chile y distinguir la convergencia formal de las capacidades efectivas de implementación. Asimismo, el análisis documental posibilitó integrar normas jurídicas, doctrina especializada e informes institucionales para examinar tanto la configuración normativa como los desafíos derivados de su aplicación.

El estudio se limita al análisis normativo y documental de Paraguay y Chile, utilizando el GDPR como parámetro internacional. Debido a que la Ley N.º 7593/2025 se encuentra en una etapa de transición previa a su entrada en vigor, no fue posible evaluar empíricamente su eficacia institucional ni su aplicación práctica.

Asimismo, la investigación no incorpora otros ordenamientos latinoamericanos ni evidencia obtenida mediante entrevistas o estudios de caso. Futuras investigaciones podrán evaluar el desempeño de la autoridad paraguaya, la aplicación del régimen sancionatorio y la respuesta institucional frente a nuevas brechas de seguridad.

CONCLUSIONES

El análisis evidencia que la Ley N.º 7593/2025 representa un avance sustancial respecto del régimen sectorial establecido por la Ley N.º 6534/2020 y aproxima formalmente a Paraguay al GDPR y al modelo chileno. No obstante, la crisis de ciberseguridad de 2025 demostró que la existencia de una legislación general no garantiza por sí sola una protección efectiva de los datos personales.

La consolidación del nuevo régimen dependerá de la autonomía funcional y presupuestaria de la autoridad de control, de su capacidad de supervisión y sanción y de la incorporación efectiva de mecanismos de responsabilidad proactiva, protección de datos desde el diseño, evaluación de riesgos y notificación de brechas. También será necesario fortalecer la coordinación entre las autoridades de protección de datos y los organismos responsables de la ciberseguridad.

En consecuencia, Paraguay ha dado un paso normativo decisivo para superar la fragmentación existente, pero todavía debe transformar las garantías legales previstas en capacidades institucionales, técnicas y operativas que aseguren una tutela efectiva de los derechos fundamentales en el entorno digital.

Declaración sobre el uso de inteligencia artificial

La autora declara haber utilizado ChatGPT, desarrollado por OpenAI, exclusivamente como herramienta de apoyo para cuestiones de formato, revisión de redacción y organización del texto, así como para asistir en la revisión posterior de las comparaciones previamente elaboradas. La selección y verificación de las fuentes, la definición de las categorías de análisis, la interpretación jurídica, los hallazgos y las conclusiones fueron realizados y validados por la autora, quien asume plena responsabilidad por el contenido del artículo.

REFERENCIAS

Constitución Política de la República de Chile. (1980). https://www.bcn.cl/leychile/navegar?idNorma=242302

European Union Agency for Cybersecurity. (2024). *ENISA threat landscape 2024*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

Greenleaf, G. (2023). Global data privacy laws 2023: 162 national laws and 20 bills. *Privacy Laws & Business International Report*, *181*, 1–4. https://doi.org/10.2139/ssrn.4426146

Kuner, C., Bygrave, L. A., Docksey, C., & Drechsler, L. (Eds.). (2020). *The EU General Data Protection Regulation (GDPR): A commentary*. Oxford University Press.

Ley N.º 19.628, Sobre protección de la vida privada. (1999). https://www.bcn.cl/leychile/navegar?idNorma=141599

Ley N.º 21.663, Ley Marco de Ciberseguridad. (2024). https://www.bcn.cl/leychile/navegar?idNorma=1202434

Ley N.º 21.719, Regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales. (2024). https://www.bcn.cl/leychile/navegar?idNorma=1209272

Ley N.º 6534/2020, De Protección de Datos Personales Crediticios. https://www.csj.gov.py/cache/lederes/G-211-28102020-L-6534.pdf

Ley N.º 7593/2025, De Protección de Datos Personales en la República del Paraguay. https://silpy.congreso.gov.py/web/ley/146223

Ministerio de Tecnologías de la Información y Comunicación. (2025a, 26 de marzo). *MITIC informa sobre presunta filtración de datos sensibles*. https://mitic.gov.py/mitic-informa-sobre-presunta-filtracion-de-datos-sensibles/

Ministerio de Tecnologías de la Información y Comunicación. (2025b, 19 de mayo). *MITIC informa sobre respuesta ante incidentes de ciberseguridad*. https://mitic.gov.py/mitic-informa-sobre-respuesta-ante-incidentes-de-ciberseguridad/

Reglamento Unión Europea 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32016R0679

Resecurity. (2025, 13 de junio). *Paraguay is being targeted by cybercriminals: 7.4 million citizen records for sale*. https://www.resecurity.com/blog/article/paraguay-is-being-targeted-by-cybercriminals-74-million-citizen-records-for-sale

TEDIC. (2025, 28 de noviembre). *La ley sobre la protección de datos personales en Paraguay: un logro colectivo basado en evidencia y participación plural*. https://www.tedic.org/la-ley-sobre-la-proteccion-de-datos-personales-en-paraguay-un-logro-colectivo-basado-en-evidencia-y-participacion-plural/