
Vacíos Normativos Y Victimización Digital De Menores Durante El Año 2025 De Redes Sociales A Dark Web En Paraguay

Regulatory Gaps And Digital Victimisation Of Minors In 2025 From Social Media To The Dark Web In Paraguay

Nathalia Vanessa Quiñonez Ruiz

Universidad del Norte, Caacupé, Paraguay

 <https://orcid.org/0009-0007-6710-0160>

nathaliaquinonezpy@gmail.com

Conflictos de interés: ninguno que declarar

Recibido: 19-02-2026

Aceptado: 02-06-2026

Vol. 6. N° 2, julio-diciembre

Resumen

El estudio analiza los vacíos normativos y la victimización digital infantil de niños, niñas y adolescentes en Paraguay durante 2025, provocada por el acceso temprano y sin controles a plataformas digitales. Este fenómeno vincula redes sociales convencionales con entornos anónimos de la dark web y fomenta la impunidad en delitos como el grooming, la sextorsión, creación y difusión o tenencia de material de abuso sexual infantil (CSAM). El objetivo general consistió en indagar de qué modo el acceso sin restricciones de niños, niñas y adolescentes a plataformas digitales incide en su victimización por ciberdelitos en Paraguay durante 2025, y examinar en qué medida los vacíos normativos constituyen un factor agravante estructural que favorece la impunidad y facilita la transición hacia la dark web, mediante un estudio dogmático-documental basado en fuentes abiertas. Los hallazgos evidencian que la ausencia de mecanismos efectivos de verificación de edad y la limitada responsabilidad de las plataformas resultan altamente agravantes al permitir la exposición precoz y la progresión hacia entornos de alta impunidad. Sin embargo, se identificaron desafíos relacionados con la subnotificación sistemática, las dificultades probatorias inherentes a los delitos cibernéticos, el estigma social y el rezago normativo frente a países como Brasil y Argentina. Los resultados confirman que el acceso sin restricciones cataliza la victimización digital infantil en línea y los vacíos normativos actúan como agravante estructural que promueve la impunidad y facilita la escalada hacia la dark web.

Palabras clave: victimización digital infantil, vacíos normativos, ciberdelitos contra NNA, grooming y sextorsión, dark web, Paraguay.

Abstract

The study examines regulatory gaps and the online victimization of children and adolescents in Paraguay in 2025, caused by early and unregulated access to digital platforms. This phenomenon links conventional social media with anonymous environments on the dark web and fosters impunity for crimes such as grooming, sextortion, and the creation, distribution, or possession of child sexual abuse material (CSAM). The overall objective was to investigate how children's and adolescents' unrestricted access to digital platforms affects their victimization by cybercrimes in Paraguay during 2025, and to examine the extent to which regulatory gaps constitute a structural aggravating factor that fosters impunity and facilitates the transition to the dark web, through a doctrinal-documentary study based on open sources. The findings show that the lack of effective age verification mechanisms and the limited accountability of platforms are major contributing factors, as they enable early exposure and progression toward environments characterized by high levels of impunity. However, challenges were identified related to systematic underreporting, the evidentiary difficulties inherent in cybercrimes, social stigma, and regulatory lag compared to countries such as Brazil and Argentina. The results confirm that unrestricted access fuels online child victimization, and regulatory gaps act as a structural aggravating factor that promotes impunity and facilitates escalation toward the dark web.

Keywords: child digital victimization, regulatory gaps, cybercrimes against children and adolescents, grooming and sextortion, dark web, Paraguay.

Introducción

La expansión de las tecnologías digitales ha modificado de manera significativa las dinámicas sociales, educativas y de comunicación en Paraguay (INE, 2024). Según datos del Instituto Nacional de Estadística, en 2024 más del 81 % de la población contaba con acceso a internet, impulsado por la adopción masiva de smartphones y la reducción progresiva de los costos de conectividad. (MarketData, 2025). Este proceso se aceleró de forma notable durante la pandemia del COVID-19, lo que incrementó la exposición de los menores a entornos digitales en un contexto de supervisión parental limitada por las medidas de aislamiento social (TEDIC, 2021).

Las estadísticas oficiales del Ministerio Público reflejan un aumento en los casos atendidos relacionados con niños, niñas y adolescentes (NNA). Durante el 2025 se registraron 21.831 víctimas NNA por diversos hechos punibles (promedio de 60 por día), de los cuales 3.386 correspondieron a abuso sexual en un promedio de 9 por día (Público, s.f.). Se observa una subnotificación significativa en delitos como grooming, sextorsión y producción de material de abuso sexual infantil (CSAM), atribuible principalmente a dificultades probatorias y al estigma social asociado.

Los riesgos vinculados al uso de plataformas convencionales (Instagram, WhatsApp, TikTok) pueden progresar hacia entornos de mayor anonimato, como la dark web[A1.1], donde la investigación y persecución de estos delitos enfrenta limitaciones importantes por la escasez de herramientas efectivas de rastreo, obtención de evidencia y mecanismos de cooperación internacional (Europol, 2025).

La literatura regional reciente confirma esta tendencia. El Informe Grooming LATAM 2024-2025 señala que el 33,5 % de los NNA en América Latina reporta contactos con fines sexuales, principalmente a través de Instagram y WhatsApp. (LATAM G. , 2025). Reportes de Save the Children (2025) y ECPAT (2025) destacan un incremento en la disponibilidad de CSAM en entornos digitales tras la pandemia, y señalan que Paraguay presenta un desarrollo normativo menos avanzado en comparación con Brasil (Marco Civil da Internet) y Argentina (proyectos legislativos contra grooming).

La Constitución Nacional en sus artículos 49 y 54 (Paraguay C. d., 1992) y el Código

de la Niñez y Adolescencia, ley N° 1.680/2001, en su artículo 32 (Paraguay, Ley N° 1680/01, Código de la Niñez y la Adolescencia, 2001) establecen la obligación de protección integral de los NNA, incluyendo la prohibición de accesos no filtrados en instituciones educativas. No obstante, este marco normativo, si bien representa un importante avance en protección general, resulta insuficiente para abordar de forma integral los ciberdelitos en entornos digitales, particularmente en espacios caracterizados por alto anonimato.

Esta insuficiencia se evidencia principalmente en la ausencia de disposiciones específicas sobre verificación obligatoria de edad en plataformas digitales, la responsabilidad proactiva de los intermediarios tecnológicos y mecanismos efectivos de investigación y persecución en entornos cifrados como la dark web. Dichas limitaciones se manifiestan en la fragmentación normativa, el enfoque predominantemente reactivo y el rezago respecto a legislaciones de países vecinos como Brasil y Argentina.

Se entiende por vacío normativo la ausencia, insuficiencia o ineficacia de disposiciones legales específicas que regulen aspectos críticos para la protección de los niños, niñas y adolescentes (NNA) en el entorno digital. Este concepto, es ampliamente utilizado en la dogmática jurídica latinoamericana (Salazar, 2025), (Romero, s.f.), (UNICEF, 2025). Se operacionaliza en este estudio como la falta de regulaciones vinculantes sobre verificación obligatoria de edad en plataformas digitales, responsabilidad objetiva de los intermediarios tecnológicos y mecanismos efectivos de investigación y persecución en entornos anónimos como la dark web. Dichos vacíos se detectan principalmente mediante comparación con estándares regionales e internacionales.

Paraguay ha incorporado disposiciones progresivas en materia de ciberdelitos y protección de datos: Ley N° 1.680/2001 (Código de la Niñez y Adolescencia CNA), Ley N° 4.439/2011 (delitos informáticos), Ley N° 6.002/2017 (abuso sexual por medios tecnológicos), adhesión al Convenio de Budapest (Europa, 2023) Ley N° 7.593/2025 (Protección de Datos Personales y Estrategia Nacional de Ciberseguridad 2025-2028). Sin embargo, estas normas mantienen un carácter fragmentado y predominantemente reactivo, lo que limita su capacidad para ofrecer una protección preventiva y efectiva en el ecosistema digital.

Se entiende por factor agravante estructural la ausencia sistemática o insuficiencia de disposiciones normativas vinculantes que impidan o mitiguen de forma efectiva la victimización digital de NNA. Estos vacíos no son meras omisiones aisladas, sino condiciones institucionales que facilitan la exposición precoz, la impunidad y la escalada hacia entornos de mayor riesgo (como la dark web).

Sin embargo, la aplicación de un marco normativo más integral y preventivo en la protección digital de NNA también presenta algunos desafíos. Uno de los principales es la necesidad de una implementación adecuada de mecanismos de verificación de edad y responsabilidad de plataformas por parte de las instituciones reguladoras y tecnológicas.

Otro desafío es la necesidad de que los operadores judiciales y legisladores cuenten con un buen conocimiento de las dinámicas del ecosistema digital y sepan cómo aplicar herramientas forenses y de cooperación internacional en la persecución de ciberdelitos contra menores (Codehupy, 2025). Contar con estos conocimientos permitiría a los operadores judiciales guiar investigaciones especializadas de manera más efectiva, reducir tiempo de respuesta, mejorar la calidad de la prueba digital, aumentar las tasas de identificación y sanción de los responsables. Asimismo, facilitaría la adopción de respuestas coordinadas y estratégicas entre las distintas instituciones del sistema de justicia, contribuyendo a disminuir la impunidad estructural que caracteriza estos delitos además de ofrecer una protección más efectiva a las víctimas NNA.

Estos actores deben estar preparados para guiar investigaciones especializadas y proporcionar respuestas coordinadas y efectivas entre el Ministerio Público, el Poder Judicial, la Policía Nacional y los organismos reguladores.

Además, algunos autores han destacado la importancia de la cooperación regional y la retroalimentación institucional en la construcción de un marco normativo preventivo. Según reportes especializados (LATAM G. , 2025), la cooperación efectiva es esencial para el abordaje integral y preventivo. Esta cooperación debe ser constructiva, específica e inmediata, además debe centrarse en el proceso de fortalecimiento normativo en lugar de respuestas únicamente reactivas. Los países de la región deben recibir retroalimentación tanto de organismos internacionales como de pares regionales, y deben ser incentivados a reflexionar sobre sus propias brechas normativas.



Por otro lado, es importante destacar que la aplicación de un enfoque preventivo en la protección digital de NNA requiere de un cambio en el rol del Estado y de las plataformas, que deben actuar como facilitadores y garantes de entornos seguros en lugar de meros proveedores de servicios (Children, 2025). El Estado debe asumir un rol protagónico en el diseño, la provisión de políticas, recursos y mecanismos que fomenten la prevención, la educación digital y la colaboración interinstitucional, ya que tiene la obligación constitucional y convencional de garantizar la protección integral de los derechos de los niños, niñas y adolescentes (artículos 49 y 54 de la Constitución Nacional y Convención sobre los Derechos del Niño). Esta responsabilidad deriva de su posición como garante último de los derechos humanos, especialmente de los grupos en situación de mayor vulnerabilidad, y ante la evidencia de que la autorregulación de las plataformas ha resultado insuficiente para reducir los riesgos cibernéticos.

Asimismo, el Estado debe estar disponible para responder a las demandas de actualización normativa y fortalecimiento institucional, con el fin de cerrar los vacíos identificados y generar un ecosistema digital más seguro.

Estudios nacionales, regionales e internacionales han evidenciado la relación entre el acceso irrestricto a plataformas digitales y la victimización de niños, niñas y adolescentes. En América Latina, el Informe Grooming (LATAM G. , 2025) y el reporte “Redes que Atrapan” de Save the Children (2025) han documentado cómo la exposición temprana a redes sociales incrementa significativamente los riesgos de grooming, sextorsión y producción de CSAM. A nivel internacional, informes de (UNICEF, 2025) y (Europol, 2025) confirman esta tendencia y alertan sobre la progresión hacia entornos de mayor anonimato como la dark web.

En el contexto paraguayo, sin embargo, persiste un rezago en la investigación empírica y normativa sobre esta problemática. Como consecuencia de lo expuesto, se formula la siguiente pregunta general de investigación: ¿De qué manera el acceso sin restricciones de niños, niñas y adolescentes a redes sociales y entornos digitales incide en su victimización mediante ciberdelitos en Paraguay durante 2025, y cómo los vacíos normativos actúan como factor agravante estructural que favorece la impunidad y facilita la progresión hacia la dark web?

El objetivo general de este estudio es indagar de qué modo el acceso sin restricciones de niños, niñas y adolescentes a plataformas digitales y redes sociales incide en su victimización por ciberdelitos en Paraguay durante 2025, y examinar en qué medida los vacíos normativos constituyen un factor agravante estructural que favorece la impunidad y facilita la transición hacia la dark web, mediante un estudio dogmático-documental basado en fuentes abiertas.

La hipótesis general de este estudio es que los vacíos normativos en Paraguay actúan como factor agravante estructural que favorece la impunidad y facilita la progresión de la victimización digital hacia entornos de mayor anonimato.

Esta investigación busca contribuir al análisis académico y al debate sobre la necesidad de fortalecer el marco normativo y las capacidades institucionales para una protección más efectiva de los derechos de la niñez y adolescencia en el ámbito digital. La relevancia de este estudio radica en la necesidad de evidencia empírica para informar reformas normativas que cierren brechas en la protección digital de NNA en Paraguay.

Metodología

Este estudio dogmático-documental, de enfoque cualitativo, diseño no experimental y alcance descriptivo-analítico, examina el marco normativo paraguayo en materia de protección de niños, niñas y adolescentes, frente a la victimización digital durante el año 2025.

La técnica principal consistió en el análisis documental mediante revisión documental de fuentes abiertas primarias y secundarias: legislación paraguaya vigente y normativa internacional, estadísticas oficiales del Ministerio Público (datos consolidados enero-diciembre 2025, publicados en 2026). La selección de fuentes se realizó mediante criterios de relevancia, actualidad (posterior a 2020) y autoría institucional verificable. Se priorizaron documentos oficiales del Ministerio Público de Paraguay, informes de organismos internacionales (UNICEF, Save the Children, ECPAT, Europol) y estudios regionales (Grooming LATAM). Se excluyeron fuentes periodísticas sin respaldo oficial o datos preliminares.



El instrumento empleado fue la ficha documental estructurada, que permitió registrar sistemáticamente la fuente, fecha, tipo de documento, contenido principal (delito, vacío normativo, estadística clave), observaciones comparativas y citas textuales relevantes. Se incorporó un análisis comparado de legislaciones del Cono Sur (Argentina, Brasil, Uruguay) para identificar brechas nacionales frente a estándares regionales, con énfasis en la ausencia de verificación efectiva de edad, responsabilidad limitada de plataformas y debilidades en la persecución transfronteriza.

El análisis normativo se realizó mediante el método dogmático-hermenéutico sistemático, complementado con un enfoque teleológico. El método hermenéutico facilitó la interpretación de las normas en sus dimensiones literal, sistemática y finalista; el enfoque sistemático permitió integrar las disposiciones dentro del ordenamiento jurídico paraguayo y compararlas con el marco regional; el enfoque teleológico evaluó el grado de cumplimiento de la finalidad protectora establecida en la Constitución Nacional y el Código de la Niñez y Adolescencia.

La metodología cualitativa permitió una interpretación integrada de los vacíos legales y su relación con la vulnerabilidad de los NNA en el ecosistema digital paraguayo, sustentando la necesidad de reformas preventivas (Witker Velásquez, s.f.)

Resultados y Discusión

La dark web es una porción de internet aproximadamente 5.000 veces más grande que la web superficial (surface web), pero no es accesible mediante navegadores convencionales ni motores de búsqueda habituales. Se trata de una red cifrada que solo puede ser accedida mediante software especializado, principalmente Tor (The Onion Router), el cual rebota el tráfico a través de múltiples nodos para garantizar el anonimato de usuarios y propietarios de sitios web.

Aunque a menudo se confunden los términos, la dark web es distinta de la deep web. Mientras esta última incluye contenidos no indexados (como bases de datos privadas), la dark web es intencionalmente oculta y encriptada. En ella se encuentran foros, mercados y comunidades ocultas, donde predomina el anonimato absoluto. (SentinelOne, 2025)

Si bien es ampliamente utilizada para actividades ilícitas (distribución de CSAM, drogas, armas, etc.), también sirve como refugio para periodistas, activistas y denunciantes que necesitan protección. Por ello, presenta dos caras: un espacio de privacidad o libertad, y un entorno que favorece la impunidad de ciberdelincuentes.

En el marco de esta investigación, la dark web se delimita como el entorno anónimo donde se concentra la mayor impunidad en la producción, distribución y comercialización de material de abuso sexual infantil (CSAM), grooming avanzado y sextorsión. Su análisis se centra en su rol como destino de escalada de la victimización digital que comienza en redes sociales convencionales.

Magnitud del problema

La victimización digital de niños, niñas y adolescentes (NNA) en Paraguay se ve influida por el acceso temprano e irrestricto a plataformas digitales.

Según la Plataforma de Datos Abiertos del Ministerio Público (consolidado enero-diciembre 2025), y conforme lo observado en la tabla 1, se atendieron 21.831 víctimas NNA por diversos hechos punibles (promedio de 60 por día). De estos, 3.386 casos correspondieron a abuso sexual en niños (promedio de 9 por día) y 2.462 investigaciones por pornografía relativa a niños (producción, distribución y posesión de CSAM). Los delitos de grooming y sextorsión (abusos por medios tecnológicos) presentan una alta subnotificación, registrándose formalmente solo 11 víctimas, principalmente debido a dificultades probatorias, estigma social y complejidades en la detección. (Paraguay M. P., s.f.)

Geográficamente, los casos se concentran en los departamentos más poblados y urbanizados del país. Los departamentos con mayor número de denuncias de abuso sexual en niños durante 2025 fueron: Central: 1.233 casos; Alto Paraná: 414 casos; Asunción (Capital): 309 casos; Itapúa: 249 casos y Caaguazú: 185 casos

Le siguen con menor pero significativa incidencia San Pedro, Cordillera, Concepción, Paraguari y Amambay. Los departamentos con menor registro de casos fueron Ñeembucú y Alto Paraguay. (Paraguay M. P., s.f.)

Esta distribución muestra que la victimización se concentra en las zonas de mayor



densidad poblacional y con mayor acceso a internet, aunque el problema se presenta a nivel nacional.

La dark web facilita la difusión anónima de CSAM. En 2025, la operación internacional contra Kidflix (Europol, 2025) desmanteló una plataforma con 1.800.000 usuarios y alrededor de 91.000 videos de abuso infantil, identificando 1.400 sospechosos, pero con solo 79 arrestos.

Además, la Dirección de Estadísticas del Poder Judicial reporta 5.841 causas judiciales por abuso sexual infantil registradas entre 2020 y el primer cuatrimestre de 2025 (con 1.481 condenas firmes en ese período), lo que refleja una carga procesal sostenida y concentrada en circunscripciones como Central (1.233 casos de abuso sexual en 2025), Alto Paraná (414) y Capital/Asunción (309). (Paraguay P. J., 2025)

En Paraguay, la carencia de herramientas forenses avanzadas y capacidades de rastreo en entornos cifrados contribuye a esta brecha, conectando victimizaciones iniciales en redes convencionales con redes globales de alta impunidad.

Tabla 1

Denuncias y atenciones a víctimas por delitos contra NNA – enero a diciembre 2025 (Ministerio Público de Paraguay). [A2.1]

Categoría	Cantidad (2025)	Detalle/Notas
Víctimas totales NNA por hechos punibles varios	21.831	Incluye abuso sexual, maltrato, estupro, pornografía infantil, violencia familiar, etc. Menores de 18 años a nivel nacional.
Víctimas de abuso sexual en niños	3.386	74% menores de 14 años; 71% niñas/adolescentes; 87% cometidos por familiar/conocido. Picos mensuales en ene (316), jul (302), ago (305), set (306), oct (306).
Investigaciones por pornografía relativa a niños (CSAM)	2.462	Incluye producción, distribución y posesión. Aumento significativo vs. años previos.
Víctimas de abuso por medios tecnológicos	11	Alta subnotificación por dificultades probatorias y estigma.
Otras categorías clave	-	Maltrato bajo tutela: 1.623; Violencia familiar: 2.943; Estupro: 990; Incumplimiento deber alimentario: 7.160; Coacción sexual: 519; Femicidio (NNA): 6.

Nota: Plataforma de Datos Abiertos del Ministerio Público (Paraguay M. P., 2026)

Los datos corresponden exclusivamente a denuncias y atenciones registradas por el

Ministerio Público de Paraguay (Plataforma de Datos Abiertos, consolidados y actualizados al 28 de enero de 2026). Representan únicamente la dimensión visible del fenómeno (dark figure of crime), con subnotificación significativa, especialmente en ciberdelitos contra NNA como grooming y sextorsión, debido a factores como estigma social, temor a la revictimización, falta de detección temprana y complejidades probatorias inherentes a la naturaleza digital y anónima de estos hechos.

Causalidad y Correlación

Según se observa en la tabla 2, existe una correlación entre el acceso irrestricto a redes sociales y la victimización, según el Informe Grooming LATAM 2024-2025.

Tabla 2
Distribución de riesgos de victimización digital por plataformas convencionales en América del Sur / América Latina (basado en estudios regionales 2024-2025)

Plataforma	Riesgo Principal	% aproximado de casos / contactos iniciales	Correlación con acceso precoz / irrestricto [A3.1]	Notas clave / Fuente principal (enfoque América del Sur/LAC)
Instagram	Grooming (contacto con fines sexuales)	60-68 % de contactos iniciales	Alta	Principal vía de captación en países como Argentina, Brasil y Paraguay; facilita escalada a sextorsión.
WhatsApp	Sextorsión y difusión no consentida	Grooming inicial y retos virales riesgosos	Alta	Uso masivo en mensajería privada en el Cono Sur; alto riesgo de extorsión tras grooming inicial.
Tiktok	Grooming inicial y retos virales riesgosos	3-15 % de contactos iniciales (creciente)	Alta	Plataforma preferida por edades 9-13 en Brasil, Argentina y Paraguay.
General (todas)	Violencia sexual digital / polivictimización	60 % interactuó con desconocidos; 33% experiencias negativas	Alta	Exposición precoz (desde 8-10 años) multiplica riesgos en toda la región.

Nota: Elaboración propia basada en Grooming LATAM Informe Regional (2024-2025, encuestas anónimas en 15 países de América Latina con énfasis en el sur); y Save the Children “Redes que Atrapan” (2025, datos regionales).

La columna “Correlación con Acceso Precoz/ Irrestricto” evalúa el nivel de asociación que los estudios regionales identifican entre el acceso temprano e irrestricto de niños, niñas



y adolescentes a las plataformas (es decir, sin verificación de edad efectiva, sin controles parentales adecuados ni límites de tiempo) y el riesgo de victimización digital.

La valoración (“Alta”) se obtuvo a partir del análisis de los informes consultados, particularmente del Informe Grooming LATAM 2024-2025, donde se evidencia que:

Los menores que acceden a estas plataformas desde edades tempranas (8-13 años) y sin supervisión presentan una probabilidad significativamente mayor de recibir contactos con fines sexuales, compartir material íntimo o ser víctimas de sextorsión.

La correlación se considera “Alta” porque los estudios muestran una relación clara y consistente: a menor edad de primer acceso y menor supervisión, mayor es la exposición a riesgos y la progresión hacia victimizaciones más graves.

Esta valoración no proviene de un análisis estadístico propio (coeficiente de correlación), sino de la síntesis cualitativa y cuantitativa de los hallazgos reportados en las fuentes citadas, que destacan el acceso precoz como uno de los principales factores de riesgo en la región.

En Paraguay, Instagram concentra aproximadamente el 68 % de los contactos iniciales con fines sexuales, porcentaje similar al registrado en Argentina. Sin embargo, el nivel de impunidad es significativamente mayor debido a la ausencia de mecanismos efectivos de verificación de edad y responsabilidad obligatoria de las plataformas (Paraguay C. d., s.f.). En la misma línea, la correlación calificada como “Alta” en la tabla anterior evidencia que el acceso precoz e irrestricto multiplica exponencialmente los riesgos de grooming, sextorsión y producción de CSAM, según los estudios regionales analizados.

Gráfico 1

Hallazgos clave de estudios sobre correlación entre acceso digital irrestricto y victimización de NNA – Enfoque en América del Sur y Paraguay.

Infancia Digital 2025 – UNICEF	Violencia contra NNA en America Latina 2015-2021 UNICEF	Aumento de riesgos digitales 2025 UNICEF
Hallazgo principal: 25% acoso escolar + 10% ciberacoso Correlación: Alta- Plataformas facilitan grooming y sextorsión. Dato adicional: 33% de violencia en pareja digital.	Hallazgo principal: 33% experiencias negativas en línea. Correlación: Media- Alta- Polivictimización incluye violencia digital.	Hallazgo principal: Adicción al móvil, sexting y grooming en aumento. Correlación: Alta- Acceso temprano lo cual implica mayor exposición.

Nota: Elaboración propia basada en informes del UNICEF (2025). Datos ilustrativos de correlación entre acceso digital y victimización. (Fund, s.f.)

Marco Normativo Actual

El marco legal paraguayo en materia de protección de los NNA frente a la victimización cibernética presenta avances progresivos, aunque fragmentados y predominantemente reactivos.

La base se encuentra en la Ley N° 1.680/2.001, cuyo artículo 32 prohíbe explícitamente el acceso a internet no filtrado para NNA, exigiendo mecanismos de control y protección. Este enfoque preventivo se complementa con el ámbito penal mediante la Ley N° 4.439/2011, que incorpora al Código Penal de delitos informáticos, incluyendo la pornografía infantil (art. 140) con penas agravadas. (Paraguay, Ley N° 4439. Que modifica y amplía varios Artículos de la Ley N° 1160/97 “Código Penal”, 2011)

Posteriormente, la Ley N° 6002/2017 tipifica el abuso sexual por medios tecnológicos, sancionando grooming, sextorsión y solicitud de material íntimo. La adhesión al Convenio de Budapest a través de la Ley N° 5.994/2017 fortalece la cooperación internacional para investigar y perseguir ciberdelitos transnacionales.

Más recientemente, la Ley N° 7.593/2025 de Protección de Datos representa un avance significativo al establecer un marco integral y moderno para el tratamiento de datos personales, tanto en el sector público como privado. Esta norma refuerza la privacidad y los derechos de los NNA como titulares especialmente vulnerables, otorgándoles protección reforzada. (Paraguay, Ley N° 7593/2025)

Entre sus principales disposiciones destacan: el establecimiento de principios como licitud, lealtad, transparencia, consentimiento informado, minimización de datos y protección especial a niños, niñas y adolescentes; la creación de la Agencia Nacional de Protección de Datos Personales, entidad con autonomía funcional encargada de supervisar el cumplimiento, atender reclamos y aplicar sanciones; el reconocimiento de derechos ARCO ampliados (acceso, rectificación, cancelación, oposición), más portabilidad y revocación del consentimiento, aplicables de forma gratuita; la obligación de los responsables y encargados del tratamiento de datos de implementar medidas de seguridad adecuadas y realizar evaluaciones de impacto, especialmente cuando se trate de datos de menores.

Por su parte, la Estrategia Nacional de Ciberseguridad 2025-2028 (aprobada por



Decreto N.º 3900/2025) actualiza el Plan Nacional de Ciberseguridad de 2017 y establece las prioridades estratégicas del país para los próximos años. Sus ejes principales incluyen: fortalecimiento de la gobernanza en ciberseguridad, gestión integral de riesgos y protección de infraestructuras críticas, desarrollo de capacidades técnicas y humanas, promoción de una cultura de ciberseguridad a nivel nacional e impulso a la cooperación internacional y la actualización del marco legal.

Esta estrategia consolida el rol del Ministerio de Tecnologías de la Información y Comunicación (MITIC) como autoridad rectora y del Centro de Respuestas a Incidentes Cibernéticos del Paraguay (CERT-PY) como órgano operativo.

En conjunto, estos instrumentos observados en la figura 1, configuran un régimen normativo en evolución, pero su fragmentación, falta de articulación integral y déficits en implementación efectiva mantienen vacíos significativos y altos niveles de impunidad, demandando mayor coordinación, actualización y enfoque preventivo-proactivo.

Figura 1

Evolución cronológica del marco normativo paraguayo en ciberdelitos contra NNA – 2001 a 2025.



Nota: Elaboración propia, basada en informes de UNICEF (2025) y Save the Children (2025). Datos ilustrativos de correlación entre acceso digital y victimización. (Children, 2025)

El marco legal paraguayo ha evolucionado de forma progresiva pero fragmentada desde 2001, como se ilustra la figura 1. Aunque se han incorporado tipos penales específicos y adhesiones internacionales, persisten brechas críticas que no existen en la misma medida en vecinos del Cono Sur, agravando la victimización digital de NNA.

Como se detalla en la Tabla 5, el marco penal paraguayo cuenta con tipos penales relevantes, pero su aplicación limitada y enfoque reactivo generan una impunidad estructural

que agrava la victimización digital de NNA, especialmente en la dark web.

Tabla 3

Tipos penales relevantes en Paraguay para ciberdelitos contra niños, niñas y adolescentes (vigencia 2025).

Tipo Penal	Artículo / Ley	Descripción breve	Pena prevista	Observaciones (enfoque Paraguay)
Abuso sexual por medios tecnológicos	Art. 135 bis (Ley N° 6.002/2017)	Abuso sexual cometido mediante comunicaciones electrónicas o sistemas informáticos	Hasta 10 años de prisión	Tipificación reciente, pero alta subnotificación por dificultad probatoria
Pornografía relativa a niños	Art. 140 (modificado por Ley N° 4.439/2011)	Producción, distribución o posesión de material de abuso sexual infantil vía sistemas informáticos	De 5 a 15 años de prisión	Delito más frecuente en denuncias 2025 (2.463 casos); concentración en la ciudad capital
Acceso indebido a sistemas informáticos	Art. 174 bis (Ley N° 4.439/2011)	Ingreso no autorizado a sistemas informáticos o bases de datos	De 2 a 5 años de prisión	Utilizado en casos de obtención de datos para grooming o sextorsión; pena baja limita disuasión
Acceso indebido agravado	Art. 174 ter (Ley N° 4.439/2011)	Acceso con agravantes (ej. afectación a menores)	Hasta 8 años de prisión	Aplicación limitada en práctica por falta de tipificación específica para NNA

Nota: Elaboración propia basada en la ley N° 1.160/97 Código Penal de Paraguay (CP), modificado por ley N° 4.439/2011 y ley N° 6.002/2017 (vigente al 2025). Datos complementarios del MP (reportes 2025).

Vacíos Normativos como Factor Agravante

La ausencia de una regulación específica y vinculante dirigida a los proveedores de plataformas digitales constituye uno de los vacíos normativos más críticos en el marco paraguayo de protección de niños, niñas y adolescentes (NNA) frente a la victimización digital. En particular, no existe una disposición legal que imponga de manera obligatoria una edad mínima de acceso a redes sociales y plataformas de mensajería, acompañada de mecanismos de verificación de identidad robustos, confiables y de aplicación generalizada (por ejemplo, verificación mediante documento de identidad, reconocimiento facial o

integración con sistemas estatales de registro civil). Esta omisión permite que menores accedan sin restricciones a entornos donde se producen contactos iniciales con fines sexuales, grooming y sextorsión, facilitando la captación precoz y la escalada hacia conductas más graves.

Asimismo, el marco vigente no establece responsabilidad objetiva ni sanciones específicas para los intermediarios tecnológicos que incumplan obligaciones de moderación proactiva, detección automática y remoción inmediata de contenidos nocivos dirigidos a NNA, ni de reporte obligatorio de material de abuso sexual infantil (CSAM) detectado en sus plataformas. Esta falta de responsabilidad deja a las empresas sin incentivos legales claros para implementar filtros avanzados, auditorías independientes o protocolos de respuesta rápida, lo que perpetúa la circulación de contenidos riesgosos y la impunidad de los agresores.

En este contexto, el Proyecto de Ley de Ciberseguridad y Protección del Ciberespacio, presentado en 2025 ante el Congreso Nacional, representa un intento de abordar parte de estas brechas. La propuesta incluye obligaciones vinculantes para intermediarios tecnológicos (moderación proactiva, verificación de edad, reporte automático de CSAM), protocolos de cooperación transfronteriza y herramientas especializadas para la investigación de ciberdelitos. No obstante, al cierre del período analizado (2025), el proyecto permanece en trámite legislativo pendiente, sin sanción ni implementación efectiva, por lo que no ha generado impacto concreto en la reducción de la vulnerabilidad de los NNA.

Esta situación normativa fragmentada y predominantemente reactiva genera un alto grado de impunidad estructural. A pesar de la elevada prevalencia real de ciberdelitos contra NNA evidenciada por la subnotificación sistemática y la magnitud de casos atendidos por el Ministerio Público (21.831 víctimas NNA en 2025, con solo 11 registros formales por abuso sexual mediante medios tecnológicos, art. 135 bis del Código Penal), la ausencia de mecanismos preventivos obligatorios y de herramientas efectivas de detección y persecución limita la capacidad del Estado para prevenir, disuadir y sancionar estas conductas de manera oportuna y eficaz.

En síntesis, los vacíos normativos no constituyen meras omisiones legislativas

aisladas, sino condiciones estructurales que facilitan y perpetúan la vulnerabilidad de los NNA en el ecosistema digital. Al no existir barreras regulatorias preventivas en las etapas iniciales (acceso irrestricto y moderación insuficiente), se permite la progresión de la victimización desde plataformas convencionales (Instagram, WhatsApp, TikTok) hacia entornos de mayor anonimato y dificultad de rastreo, como la dark web. Esta dinámica se asocia directamente con la subnotificación, la dificultad probatoria y la limitada respuesta institucional, confirmando que la ausencia de regulación vinculante y proactiva que opera como un factor asociado que agrava la exposición y la impunidad en el continuum digital.

Tabla 4

Regulación de edad mínima y mecanismos de verificación en plataformas digitales – Países seleccionados de América del Sur (situación vigente al 2025-2026).

País	Edad mínima obligatoria para acceso a redes sociales	Mecanismo de verificación de edad implementado	Responsabilidad de plataformas (moderación y remoción de contenido nocivo)	Estado actual de la regulación (2025-2026)	Fuente principal / Observaciones
Paraguay	No establecida de forma obligatoria (solo recomendaciones generales en Ley 1.680/01 art. 32)	Ausente o voluntario (sin verificación estricta)	Parcial (Ley 7.593/25 de Protección de Datos y Estrategia Ciberseguridad, pero sin obligaciones específicas para plataformas)	Fragmentada y reactiva; proyecto de ley de Ciberseguridad pendiente	Ministerio Público / Leyes 1.680/01, 4.439/11, 6.002/17, 7.593/25.
Brasil	13 años (recomendada, con propuestas de endurecimiento)	Parcial (Marco Civil da Internet + moderación obligatoria)	Sí (alta responsabilidad por remoción rápida de CSAM y grooming)	Avanzada; Ley ECA Digital (2025) refuerza protección	Marco Civil da Internet / SaferNet Brasil 2025
Uruguay	14 años (propuesta legislativa en discusión desde 2024)	En proceso (proyectos de verificación obligatoria)	Parcial (Ley de Protección de Datos y normativas audiovisuales)	En trámite; avances hacia edad mínima obligatoria	Ministerio del Interior / Proyectos legislativos 2024-2025

Nota: Elaboración propia basada en legislación nacional vigente (2025-2026), informes UNICEF América Latina y el Caribe (2025), Grooming Argentina, SaferNet Brasil y análisis comparado regional (OEA/Red Latinoamericana de Protección de Datos).

La ausencia de una edad mínima obligatoria y de mecanismos de verificación estricta en Paraguay constituye, sin lugar a duda, uno de los vacíos normativos más críticos en el

Cono Sur. Esta deficiencia facilita la exposición precoz de los NNA a plataformas digitales y su posterior progresión hacia entornos de mayor riesgo como la dark web.

En contraste, otros países del Cono Sur han avanzado en regulaciones más estrictas, con efectos positivos preliminares en la protección de menores:

Brasil ha implementado el Estatuto da Criança e do Adolescente Digital (ECA Digital - Ley N° 15.211/2025), que entró en vigencia en marzo de 2026. Esta norma exige verificación de edad confiable (prohibiendo la simple autodeclaración), vinculación obligatoria de cuentas de menores de 16 años a un responsable legal, remoción rápida de contenidos de explotación sexual y la prohibición de diseños adictivos en plataformas. Los primeros reportes indican un aumento significativo en la detección y eliminación de material de abuso sexual infantil (CSAM) y mayor presión regulatoria sobre las plataformas.

Argentina mantiene la edad mínima de 13 años recomendada por las propias plataformas, pero cuenta con proyectos legislativos avanzados y una aplicación más estricta de responsabilidad de intermediarios tecnológicos. Se han fortalecido los mecanismos de reporte de CSAM y cooperación con plataformas, logrando mejores tasas de remoción de contenidos nocivos en comparación con Paraguay.

Uruguay ha avanzado en proyectos legislativos que proponen una edad mínima de 14 años y verificación obligatoria de edad, junto con mayor regulación de la responsabilidad de las plataformas en materia de moderación proactiva.

Estos ejemplos regionales demuestran que regulaciones más exigentes en verificación de edad y responsabilidad de plataformas tienden a reducir la exposición inicial de los NNA, mejorar la detección temprana de grooming y sextorsión y dificultar la escalada hacia entornos de alta impunidad. Paraguay presenta un rezago significativo frente a Brasil y, en menor medida, frente a los avances de Argentina y Uruguay, lo que agrava la vulnerabilidad de sus niños, niñas y adolescentes en el ecosistema digital.

Conclusión

El propósito de este trabajo fue indagar de qué modo el acceso sin restricciones de niños, niñas y adolescentes (NNA) a plataformas digitales y redes sociales incide en su



victimización por ciberdelitos en Paraguay durante 2025, y examinar en qué medida los vacíos normativos constituyen un factor agravante estructural que facilita la impunidad y la progresión hacia entornos de mayor anonimato como la dark web.

Los resultados muestran que el marco normativo paraguayo incorpora avances parciales, como la Ley N° 7.593/2025 de Protección de Datos Personales y la Estrategia Nacional de Ciberseguridad 2025-2028, que fortalecen aspectos de privacidad y gobernanza cibernética. No obstante, persisten debilidades en áreas clave: ausencia de edad mínima obligatoria con mecanismos de verificación efectiva, responsabilidad limitada de las plataformas digitales y capacidades insuficientes para investigar entornos anónimos o coordinar respuestas de forma ágil a nivel regional. En comparación con Brasil y Argentina, que han avanzado en disposiciones sobre moderación obligatoria y proyectos de verificación de edad, Paraguay presenta rezagos que se asocian con mayor exposición inicial y dificultades en la respuesta institucional.

Operaciones internacionales como la desarticulación de Kidflix (Europol, 2025) ilustran que la cooperación transfronteriza es viable, pero su efectividad en Paraguay depende de un fortalecimiento local mediante herramientas forenses avanzadas, unidades especializadas en ciberdelitos sexuales contra menores y mayor inversión en capacidades de rastreo y análisis digital.

Los hallazgos indican que el acceso sin restricciones al entorno digital actúa como factor facilitador de la victimización al reducir barreras protectoras en etapas críticas del desarrollo, mientras que las insuficiencias normativas contribuyen como condición estructural que limita la prevención, la detección y la sanción efectiva, generando un desequilibrio que favorece la continuidad de estas conductas.

Para abordar estas brechas y fortalecer la protección de NNA, se sugiere adoptar un enfoque preventivo e integral que contemple: la imposición de verificación de edad obligatoria y confiable en todas las plataformas digitales, acompañada de penalizaciones claras por incumplimiento; la exigencia de responsabilidad objetiva a los intermediarios tecnológicos, incorporando medidas de moderación proactiva, auditorías periódicas independientes y reporte automático de contenidos sospechosos o de material de abuso



sexual infantil (CSAM); el fortalecimiento de unidades especializadas en investigación de ciberdelitos sexuales contra menores, dotadas de herramientas forenses avanzadas capaces de operar en entornos cifrados y anónimos; y el impulso de mecanismos de cooperación regional más fluidos y operativos a través del MERCOSUR y el Convenio de Budapest, incluyendo protocolos ágiles de intercambio de información y asistencia técnica transfronteriza.

Asimismo, se recomienda implementar un sistema de seguimiento continuo mediante encuestas nacionales anuales, inspiradas en el modelo Kids Online de UNICEF, para medir indicadores clave como niveles de subnotificación, frecuencia de contactos riesgosos y eficacia de las intervenciones, permitiendo adaptar dinámicamente las políticas públicas en base a evidencia actualizada y sistemática.

Este enfoque contribuiría a transformar la conectividad digital en una oportunidad de desarrollo para la niñez y adolescencia, reduciendo su exposición a riesgos y fortaleciendo la capacidad de respuesta institucional en un ámbito en constante evolución.[A4.1]

Como continuación de este estudio, se proponen las siguientes líneas de investigación:

Realizar un estudio empírico-cuantitativo que mida el impacto real de la implementación de verificación de edad obligatoria en Paraguay, comparando tasas de victimización antes y después de su eventual aprobación.

Analizar la efectividad de la cooperación judicial y policial entre Paraguay, Brasil y Argentina en la persecución de ciberdelitos contra NNA en la dark web.

Investigar el rol de la educación digital y los controles parentales como factores protectores en contextos de alto rezago normativo.

Estudiar el impacto de la inteligencia artificial en la detección automatizada de grooming y CSAM en plataformas utilizadas por menores paraguayos.

Referencias Bibliográficas

- Children, S. t. (2025). *Redes que atrapan: La explotación sexual de la infancia y la adolescencia en entornos digitales*. Obtenido de https://www.savethechildren.es/sites/default/files/2025-07/Redes_que_atrapan_STC.pdf
- Codehupy. (2025). *Derechos Humanos en Paraguay 2025*. Obtenido de https://www.tedic.org/wp-content/uploads/2026/01/Informe-DDHH-2025_web.pdf
- Europa, C. d. (2023). *Convenio sobre la ciberdelincuencia* (Budapest Convention on Cybercrime). Obtenido de Consejo de Europa: <https://www.coe.int/documents/8475493/202017550/PREMS+015123+ESP+2023+Convention+Cybercrimiminalite%CC%81+WEB+A5.pdf/a6b85c77-c79a-ef99-4d66-48351c1b48fc?t=1678890134243>
- Europol. (2025). *Operación contra Kidflix: Desmantelamiento de plataforma con 1.8 millones de usuarios*. Obtenido de <https://www.elimparcial.com/mundo/2025/04/03/desmantelada-kidflix-una-de-las-mayores-plataformas-de-pedofilia-del-mundo-en-operacion-internacional-39-ninos-en-situacion-de-explotacion-han-sido-rescatados/>
- Fund, U. N. (s.f.). *Publicaciones*. Obtenido de <https://www.unicef.org/es/informes>
- INE. (2024). *Microdatos*. Obtenido de <https://www.ine.gov.py/noticias/2436/8-de-cada-10-personas-utiliza-internet-en-paraguay>
- LATAM, G. (2025). *Informe 2024-2025 Grooming LATAM*. Obtenido de <https://www.groominglatam.org/wp-content/uploads/2025/05/INFORME-2024-2025-GROOMING-LATAM.pdf>
- LATAM, L. R. (2025). *Informe 2024-2025 Grooming LATAM [PDF]*. Obtenido de <https://www.groomingarg.org/wp-content/uploads/2025/05/INFORME-2024-2025-GROOMING-LATAM.pdf>
- MarketData. (24 de Junio de 2025). *Acceso a internet en Paraguay alcanza al 81,6% de la población: ¿Quiénes lo usan más, dónde y para qué?* Obtenido de <https://marketdata.com.py/educacion/tecnologia/acceso-a-internet-en-paraguay-alcanza-al-816-de-la-poblacion-quienes-lo-usan-mas-donde-y-para-que-143217>
- Paraguay. (2001). *Ley N° 1680/01, Código de la Niñez y la Adolescencia*. Obtenido de



- Biblioteca y Archivo Central del Congreso Nacional: <https://www.bacn.gov.py/leyes-paraguayas/5261/ley-n-1680-codigo-de-la-ninez-y-la-adolescencia>
- Paraguay. (2011). *Ley N° 4439. Que modifica y amplía varios Artículos de la Ley N° 1160/97 “Código Penal”*. Obtenido de Sistema de Información Legislativa (SILPY), Congreso Nacional del Paraguay: https://www.unodc.org/cld/es/document/pry/2011/ley_4439_de_2011.html
- Paraguay. (2017). *Ley N° 5994/2017. Que aprueba la Convención sobre la Ciberdelincuencia, y el Protocolo Adicional al Convenio sobre Ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos*. Obtenido de: <https://www.bacn.gov.py/leyes-paraguayas/9900/ley-n-5994-aprueba-la-convencionsobre->
- Paraguay. (2017). *Ley N° 6002/2017. Que modifica el artículo 135 de la Ley N° 1160/97 “Código Penal”*. Obtenido de Sistema de Información Legislativa (SILPY), Congreso Nacional del Paraguay: <https://silpy.congreso.gov.py/web/ley/138814>
- Paraguay. (2025). *Ley N° 7593/2025. De Protección de Datos Personales en la República del Paraguay*. Obtenido de Sistema de Información Legislativa (SILPY), Congreso Nacional del Paraguay: <https://silpy.congreso.gov.py/web/ley/146223>
- Paraguay, C. d. (1992). Constitución Nacional (versión actualizada 2022 UV). Obtenido de Honorable Cámara de Senadores: <https://odd.senado.gov.py/archivos/file/Constitucion%20Nacional%20UV%202022.pdf>
- Paraguay, C. d. (s.f.). *El uso de Instagram en los paraguayos*. Obtenido de Revista CAP: <https://revistacap.com.py/2022/07/06/el-uso-de-instagram-en-los-paraguayos/>
- Paraguay, M. P. (28 de Enero de 2026). *Datos Abiertos: De enero a diciembre del año 2025, el Ministerio Público atendió un total de 21.831 niños, niñas y adolescentes víctimas de diferentes hechos punibles, 60 por día*. Obtenido de Plataforma de Datos Abiertos: <https://www.ministeriopublico.gov.py/nota/datos-abiertos-de-enero-a-diciembre-del-ano-2025-el-ministerio-publico-atendio-16082>
- Paraguay, M. P. (s.f.). *Página principal*. Obtenido de <https://www.ministeriopublico.gov.py/nota/datos-abiertos-de-enero-a-diciembre-del-ano-2025-el-ministerio-publico->

atendio-un-total-de-21831-ninos-ninas-y-adolescentes-victimas-de-diferentes-hechos-punibles-60-por-dia-16082

Paraguay, P. J. (Mayo de 2025). *Estadísticas del Poder Judicial reportan más de 5.800*

causas judiciales por abuso sexual infantil [Página web]. Obtenido de <https://www.pj.gov.py/notas/28089-estadisticas-del-poder-judicial-reportan-mas-de-5800-causas-judiciales-por-abuso-sexual-infantil?referrer>

Público, M. (s.f.). *Ministerio Público - Fiscalía General del Estado*. Obtenido de [https://](https://www.ministeriopublico.gov.py/buscar?b=Datos+consolidados+enero-diciembre+2025)

www.ministeriopublico.gov.py/buscar?b=Datos+consolidados+enero-diciembre+2025

Romero, J. (s.f.). *Derechos de niños, niñas y adolescentes en entornos digitales: desafíos*

regulatorios en América Latina. Obtenido de Asesoría Técnica Parlamentaria, Biblioteca del Congreso Nacional de Chile. Informe N.º 143079: https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio%2F10221%2F36851%2F2%2FBCN_NNA_Digital_VF_pdf.pdf&utm

Salazar, S. (2025). *Ciudadanía digital y vacíos normativos en la protección de la infancia*

latinoamericana. Obtenido de Instituto Interamericano del Niño, Niña y Adolescente (IIN-OEA): https://issuu.com/institutointeramericanodelninolanin/docs/estado_de_situaci_n_sobre_la_legislaci_n_y_pol_tic?utm_source=copilot.com

SentinelOne. (1 de Mayo de 2025). *Qué es la dark web? Todo lo que debes saber*. Obtenido de <https://www.sentinelone.com/es/cybersecurity-101/threat-intelligence/what-is-the-dark-web/>

TEDIC. (2021). *Memoria 2020*. Obtenido de [Informe anual]: <https://www.tedic.org/wp-content/uploads/2021/06/Memoria-TEDIC-2020-ES.pdf>

UNICEF. (2025). *Infancia, adolescencia y bienestar digital: una aproximación desde la salud, la convivencia y la responsabilidad social*. Obtenido de UNICEF España, Universidad de Santiago de Compostela y Consejo General de Colegios de Ingeniería Informática : https://www.unicef.es/publicacion/infancia-adolescencia-y-bienestar-digital?utm_

Witker Velásquez, J. A. (s.f.). *Perfil del investigador: Witker Velásquez, Jorge Alberto*.

Obtenido de Instituto de Investigaciones Jurídicas, Universidad Nacional Autónoma de México.: <https://www.juridicas.unam.mx/investigador/perfil/witker>

