

Obligatoriedad parental y protección de la identidad virtual de niños, niñas y adolescentes

Parental Obligations and the Protection of Children's and Adolescents' Virtual Identity



DOI: <https://doi.org/10.33324/dicere.v3i1.1097>

Marcela Paz Sánchez-Sarmiento,  <https://orcid.org/0000-0002-8927-5478>  msanchezs@ucacue.edu.ec
Universidad Católica de Cuenca, Cuenca, Ecuador.

Recibido: 28-02-2026 **Revisado:** 07-05-2026 **Aceptado:** 19-05-2026 **Publicado:** 30-05-2026

Resumen

El artículo examina si la parentalidad en el entorno digital puede justificar la exposición discrecional de niñas, niños y adolescentes o si, por el contrario, se encuentra jurídicamente limitada por un deber reforzado de protección. Mediante un análisis jurídico-doctrinal, hermenéutico y comparado, se estudian la Constitución ecuatoriana, la Ley Orgánica de Protección de Datos Personales, su Reglamento General, la norma general de 2026 sobre actividades familiares o domésticas, el Código de la Niñez y Adolescencia y los estándares internacionales aplicables. La tesis sostenida es que madres, padres y

representantes no tienen libre disposición sobre huellas digitales, imagen, voz, geolocalización, salud, datos escolares o perfiles conductuales de sus hijos, sino que actúan como garantes fiduciarios sometidos al interés superior, la autonomía progresiva, la minimización y la responsabilidad demostrada. La contribución del trabajo consiste en vincular esos principios con la regla ecuatoriana de excepción doméstica y proponer un test de juridicidad para publicaciones parentales, *sharenting* y prácticas de influencia familiar.

Abstract

This article examines whether parental authority in digital environments may justify the discretionary exposure of children and adolescents, or whether it is limited by a reinforced duty of protection. Through doctrinal, hermeneutic and comparative legal

analysis, it studies the Ecuadorian Constitution, the Organic Law on Personal Data Protection, its General Regulation, the 2026 general rule on family or domestic data processing, the Code on Children and Adolescents, and international standards such as

the Convention on the Rights of the Child, General Comment No. 25 and the American Convention on Human Rights. It argues that parents and legal representatives do not have free disposal over children's digital traces, image, voice, geolocation, health, school or behavioral data; rather, they act as fiduciary guarantors bound by the best

interests of the child, progressive autonomy, minimization and accountability. The article's contribution is to connect those principles with Ecuador's recent domestic-exemption rule and to propose an operational legality test for parental publication, *sharenting* and *family influencing* practices.

Palabras clave

derechos de la niñez, protección de datos personales, *sharenting*, identidad virtual, Ecuador

Keywords

children's rights, personal data protection, *sharenting*, virtual identity, Ecuador

1 Introducción

La protección de los niños, niñas y adolescentes (en adelante, NNA) en el entorno digital exige revisar los límites jurídicos de la exposición parental. La transformación digital ha trasladado parte relevante de la vida familiar a espacios de circulación, archivo y monetización permanentes: fotografías de nacimientos, videos de rutinas, diagnósticos médicos, logros escolares, localización en tiempo real y relatos íntimos de crianza pueden publicarse, replicarse y reutilizarse con una facilidad inédita. Como ha advertido la literatura sobre derechos de la niñez en entornos digitales, la vida en línea no constituye una esfera marginal, sino un ámbito ordinario de realización y afectación de derechos (Livingstone & Third, 2017; Comité de los Derechos del Niño, 2021). En ese contexto, el problema jurídico central no consiste solo en determinar cuándo acceden los NNA a plataformas digitales, sino bajo qué límites

pueden sus propios progenitores construir, administrar o explotar su presencia en línea antes de que ellos puedan intervenir plenamente en esa decisión.

La particularidad de este trabajo reside en desplazar el análisis desde el debate general sobre privacidad infantil hacia una tesis específica de derecho ecuatoriano: la parentalidad digital debe operar como función fiduciaria de custodia de una identidad ajena en formación. A diferencia de estudios comparados centrados en España, Italia, Argentina o Chile, aquí se integra el régimen ecuatoriano de protección de datos personales, su Reglamento y la Norma General de 2026 sobre actividades familiares o domésticas para demostrar que el origen familiar de la publicación no basta para excluir el control jurídico cuando existen difusión pública, finalidad comercial o afectación de derechos.

Sobre esa base, la Ley Orgánica de Protección de Datos Personales (LOPDP, 2021) introdujo un régimen específico para el tratamiento de datos de NNA, reconociéndolos como categoría especial de datos y consagrando, entre otros, el derecho a no ser objeto de decisiones basadas única o parcialmente en valoraciones automatizadas, la educación digital y reglas reforzadas para el ejercicio de derechos según la edad y madurez del titular (arts. 21-25). El Reglamento General a la LOPDP definió además las actividades familiares o domésticas como aquellas desarrolladas en un entorno de amistad, parentesco o grupo personal cercano, en propiedad privada y sin finalidad de comunicación o transferencia con fines comerciales (Presidencia de la República del Ecuador, 2023, art. 4). Esta cláusula, que parecía reservar una zona inmune al control del derecho de datos, ha sido concretada por la Superintendencia de Protección de Datos Personales (SPDP), que en 2026 estableció que la difusión a un número indeterminado de personas, el uso comercial o el impacto lesivo en derechos fundamentales hacen perder el carácter familiar o doméstico del tratamiento (SPDP, 2026a, arts. 4-6).

La literatura comparada ha denominado *sharenting* al fenómeno consistente en compartir en línea información, imágenes o relatos sobre hijos e hijas por parte de madres, padres o cuidadores (Blum-Ross & Livingstone, 2017; Steinberg, 2017). Aunque esta práctica puede responder a motivaciones afectivas, de memoria familiar, búsqueda de apoyo o afirmación identitaria adulta, sus efectos sobre la privacidad, la autonomía futura, la reputación y la seguridad de NNA son significativos. Estudios empíricos muestran que muchas personas menores de edad desean ser consultadas antes de que sus imágenes o experiencias sean publicadas, y que perciben determinadas exposiciones como embarazosas, inútiles o conflictivas con la identidad que

buscan construir por sí mismas (Ouvrein & Verswijvel, 2019; Sarkadi et al., 2020).

En el ordenamiento ecuatoriano, la parentalidad digital no confiere un poder de libre disposición sobre los datos personales y la identidad virtual de NNA, sino una obligación reforzada de protección. Dicha obligación deriva de la concurrencia entre interés superior, responsabilidad parental, autonomía progresiva y protección de datos personales, y exige a los representantes legales actuar bajo criterios de necesidad, proporcionalidad, minimización, escucha activa y prevención del daño. En consecuencia, cuando la exposición parental excede el entorno íntimo o persigue fines de visibilidad pública, influencia comercial o monetización, la conducta debe ser examinada bajo los parámetros ordinarios de licitud, lealtad, finalidad y responsabilidad del derecho de datos, sin ampararse en la excepción doméstica.

De esta manera, este trabajo parte de una hipótesis precisa: en el ordenamiento ecuatoriano, la parentalidad digital no autoriza una libre disposición sobre los datos personales y la identidad virtual de NNA, sino que activa una obligación reforzada de custodia; por ello exige decisiones guiadas por necesidad, proporcionalidad, minimización, escucha y prevención del daño. Con ese punto de partida, esta investigación busca compeler el contenido jurídico de dicha obligación y sus consecuencias prácticas en Ecuador. Para ello delimita el concepto de identidad virtual de NNA, sistematiza el marco constitucional, familiar y de protección de datos, integra estándares internacionales y comparados, examina los riesgos del *sharenting* y del *family influencing*, y propone un test de juridicidad para la actuación parental en entornos digitales.

2 Metodología y marco conceptual

La investigación se desarrolla desde una metodología jurídico-doctrinal con apoyo hermenéutico y comparado. El análisis no se limita a una lectura aislada de disposiciones, sino que reconstruye la relación entre la Constitución de la República del Ecuador (CRE), el Código de la Niñez y Adolescencia (CNA), la LOPDP, su Reglamento General y la normativa secundaria de la Superintendencia de Protección de Datos Personales de Ecuador, atendiendo a sus principios, finalidades y puntos de contacto. Junto a ello, se incorporan estándares internacionales y literatura especializada sobre *sharenting*, autonomía progresiva y derechos de la niñez en el entorno digital. El objetivo metodológico es doble: extraer consecuencias normativas para el derecho ecuatoriano vigente y, al mismo tiempo, ofrecer criterios de aplicación para supuestos en los que la exposición parental aparece como práctica cotidiana o como actividad con proyección pública o comercial.

Para fortalecer la trazabilidad metodológica, el corpus bibliográfico se seleccionó mediante búsqueda dirigida en bases y repositorios académicos y jurídicos, incluyendo Scopus, Web of Science, SciELO, Redalyc, Dialnet, HeinOnline, Google Scholar y portales oficiales de autoridades de protección de datos, con prioridad en trabajos publicados entre 2017 y 2026. Se incluyeron fuentes que abordaran derechos de la niñez en entornos digitales, protección de datos personales, *sharenting*, responsabilidad parental, autonomía progresiva, derecho a la imagen y remedios frente a la sobreexposición. Se excluyeron textos meramente divulgativos sin respaldo normativo o empírico, salvo cuando provenían de autoridades públicas y eran útiles para identificar directrices recientes. El componente comparado se utiliza con función persuasiva y no trasplantativa:

permite contrastar tendencias regulatorias sin desplazar el análisis del derecho ecuatoriano vigente.

2.1. Identidad virtual de NNA como objeto de tutela jurídica

La categoría “identidad virtual” no siempre aparece formulada de manera expresa en los textos normativos, pero puede ser reconstruida dogmáticamente como el conjunto de signos, datos, representaciones, trazas y perfiles que permiten individualizar, describir, anticipar o reputar a una persona en el entorno digital (OEA, 1969). En el caso de NNA, esa identidad comprende, al menos, su nombre, imagen, voz, rasgos biométricos, ubicación, vínculos familiares, rutinas, hábitos de consumo, escolaridad, salud, comportamiento observable, historial comunicacional, reputación en línea y metadatos asociados a sus interacciones (Naciones Unidas, 1989). No se reduce, por tanto, a una fotografía: incluye la huella digital acumulativa que terceros pueden tratar, reutilizar, perfilar o combinar.

Desde una perspectiva jurídica, la identidad virtual de NNA se sitúa en la intersección de varios derechos: identidad, intimidad, honor, imagen, autodeterminación informativa, libre desarrollo de la personalidad, igualdad y no discriminación. El Convenio sobre los derechos del Niño (CDN) prohíbe toda injerencia arbitraria o ilegal en la vida privada, familia, domicilio o correspondencia del niño, así como los ataques ilícitos a su honra y reputación (Naciones Unidas, 1989, art. 16). La CADH, de modo convergente, reconoce el derecho al honor, la dignidad y la protección contra interferen-

cias arbitrarias o abusivas en la vida privada, la vida familiar, el domicilio y la correspondencia (Organización de los Estados Americanos [OEA], 1969, art. 11). En el plano interno, la CRE y el CNA reproducen y refuerzan ese haz de garantías (CRE, 2008, art. 66 num. 18-21; Congreso Nacional del Ecuador, 2003, arts. 51, 53). Esta tendencia normativa permite sostener que la identidad virtual de NNA no es un interés accesorio, sino una manifestación concreta de derechos personalísimos que requiere tutela preventiva frente a tratamientos acumulativos y difícilmente reversibles.

La utilidad analítica del concepto radica en que permite desplazar el enfoque desde la foto aislada hacia la estructura relacional del riesgo digital. Una imagen de un niño en uniforme escolar puede revelar centro educativo, edad aproximada, trayecto cotidiano, entorno socioeconómico y círculos de sociabilidad; un video doméstico puede exponer datos de salud, estilo de crianza, estructura familiar o vulnerabilidades emocionales; una publicación aparentemente trivial puede quedar indexada, replicada por terceros o utilizada para entrenamiento algorítmico, perfilamiento comercial, acoso, fraude o explotación sexual. Por ello, la identidad virtual de NNA debe ser entendida como un bien jurídico relacional, progresivo y particularmente frágil.

La noción de identidad virtual debe comprenderse también como identidad digital creada por terceros. Berg et al. (2024) coinciden, en una revisión de alcance sobre niños desde la concepción hasta los ocho años, dos formas relevantes de configuración identitaria en redes: la identidad digital social, asociada a memoria familiar y comunicación, y la identidad digital performativa, vinculada a exposición pública y reputacional. Esta distinción refuerza que el problema jurídico no se limita a la publicación aislada, sino a la construcción acumulativa de perfiles, narrativas y expectativas sociales sobre una persona que aún

no controla plenamente su autorrepresentación.

De esta manera, la tipología revisada de riesgos de la OCDE exige no reducir la discusión a privacidad en sentido estrecho. Los riesgos de contenido, contacto, conducta y consumo se entrecruzan con riesgos transversales de privacidad, tecnologías avanzadas y bienestar, lo que permite explicar por qué una publicación parental puede generar simultáneamente exposición reputacional, contacto no deseado, explotación comercial y reutilización algorítmica (OCDE, 2025).

2.2. De la patria potestad a la responsabilidad parental digital

En el derecho de familia contemporáneo, la relación paterno-filial no puede concebirse como un espacio de dominio sobre la persona menor de edad, sino como una función orientada a su cuidado, desarrollo y protección. El Código de la Niñez y Adolescencia (CNA) es claro al atribuir al padre y a la madre una responsabilidad compartida de respeto, protección y cuidado, junto con la promoción y exigibilidad de los derechos de sus hijos (Congreso Nacional del Ecuador, 2003, art. 9). El interés superior del niño, además, obliga a todas las autoridades e instituciones públicas y privadas a ajustar sus decisiones y acciones al ejercicio efectivo de sus derechos, y prohíbe invocarlo sin escuchar previamente la opinión del niño, niña o adolescente cuando esté en condiciones de expresarla (Congreso Nacional del Ecuador, 2003, art. 11).

Trasladado al entorno digital, ello significa que la representación legal no equivale a una licencia para exponer discrecionalmente a NNA en redes sociales. La parentalidad digital debe ser comprendida como una forma específica de responsabilidad parental: una función fiduciaria de gestión

prudente de la información ajena, sometida a fines de protección y al deber de evitar que decisiones presentes comprometan la autonomía, seguridad y reputación futuras del titular. La CDN refuerza esta interpretación al reconocer las responsabilidades, derechos y deberes de madres, padres o representantes para orientar al niño de un modo consistente con la evolución de sus facultades (Naciones Unidas, 1989, art. 5). La orientación parental es, entonces, instrumental al ejercicio de derechos del hijo, no sustitutiva indefinida de su personalidad digital.

En este punto, resulta crucial distinguir entre representación y apropiación. La primera constituye una función jurídica de garantía, orientación y defensa de derechos del niño, niña o adolescente, ejercida conforme al interés superior, la evolución progresiva de sus facultades y la finalidad protectora de la patria potestad; por ello, en el ordenamiento ecuatoriano, la patria potestad no se configura únicamente como un conjunto de derechos de los padres, sino también como obligaciones relativas al cuidado, educación, desarrollo integral

y defensa de los derechos y garantías de los hijos (Congreso Nacional del Ecuador, 2003). Además, cuando exista conflicto de intereses entre el hijo y quien ejerce la representación legal, esta puede suspenderse, lo que confirma que la representación no es una facultad de disposición sobre la esfera jurídica del NNA. La apropiación, en cambio, supone tratar la identidad, imagen, voz, intimidad, datos personales, reputación o presencia digital del hijo como una prolongación disponible del proyecto expresivo, comercial o reputacional del adulto, en tensión con los derechos propios del NNA a la identidad, dignidad, imagen, privacidad, honra, reputación, protección de datos personales y correspondencia física o virtual (CRE, 2008). El giro del derecho de familia hacia la protección integral y la autonomía progresiva excluye esa segunda lectura. En consecuencia, la pregunta jurídicamente relevante no es si la publicación proviene de los padres, sino si la actuación es necesaria, proporcional, segura, reversible y consistente con el interés superior y la dignidad digital del NNA.

3 Marco normativo ecuatoriano aplicable

El marco ecuatoriano ofrece una base particularmente robusta para reconducir la exposición digital parental desde la lógica de la potestad hacia la lógica del deber. Esa base no se agota en la LOPDP, sino que integra normas constitucionales, disposiciones de niñez y adolescencia y desarrollo reglamentario reciente.

3.1. Constitución: intimidad, datos personales e interés superior

La CRE reconoce el derecho al honor y buen nombre y dispone que la ley protegerá la imagen y la voz de la persona (CRE, 2008, art. 66 num. 18). Asimismo, consagra el derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de ese carácter, y exige autorización del titular o mandato legal para su recolección, archivo, procesamiento, distribución o difusión (CRE, 2008, art. 66 num. 19). A ello se suman el derecho a la intimidad personal y familiar y la invio-

labilidad y secreto de la correspondencia física y virtual (CRE, 2008, art. 66 num. 20-21).

En el caso de NNA, estos derechos se intensifican por la cláusula de protección reforzada del artículo 44 constitucional. Allí se impone al Estado, la sociedad y la familia el deber de promover prioritariamente el desarrollo integral y asegurar el ejercicio pleno de derechos, bajo el principio de interés superior y con prevalencia sobre los derechos de las demás personas (CRE, 2008, art. 44). De esta disposición se deriva una consecuencia de primer orden: la libertad expresiva, reputacional o comercial de los progenitores no puede prevalecer automáticamente frente al interés del hijo a conservar un ámbito de reserva y a construir, en el futuro, su propia identidad digital.

3.2. Código de la Niñez y Adolescencia: familia, privacidad y participación

El CNA aporta tres ejes de lectura que resultan decisivos. De un lado, reconoce y protege a la familia como espacio natural y fundamental para el desarrollo integral del niño, niña y adolescente, y asigna prioritariamente a padre y madre la responsabilidad compartida del respeto, protección y cuidado de sus hijos, así como la promoción y exigibilidad de sus derechos (Congreso Nacional del Ecuador, 2003, art. 9). De otro, impone que toda decisión se oriente por el interés superior, sin prescindir de la opinión de la persona menor de edad cuando pueda expresarla (Congreso Nacional del Ecuador, 2003, art. 11). Finalmente, tutela de manera expresa la intimidad de la vida privada y familiar, así como la privacidad e inviolabilidad de domicilio, correspondencia y comunicaciones telefónicas y electrónicas (Congreso Nacional del Ecuador, 2003, art. 53).

Leído en clave digital, este régimen impide tratar la presencia en línea del hijo como un ámbito disponible de forma unilateral. El derecho a ser consultado en los

asuntos que le afecten y a que su opinión sea ponderada según su edad y madurez (Congreso Nacional del Ecuador, 2003, art. 60) obliga a descartar prácticas parentales que presuponen una cesión silenciosa de imagen, relato vital o datos personales. La consulta no es una cortesía familiar; es una exigencia jurídica de consideración progresiva.

3.3. LOPDP: régimen reforzado para datos de NNA

La LOPDP, publicada en 2021, constituye el eje específico del análisis. La ley no es aplicable, en principio, a personas naturales que utilicen datos en la realización de actividades familiares o domésticas (Asamblea Nacional del Ecuador, 2021, art. 2 lit. a). Sin embargo, esa exclusión debe ser interpretada restrictivamente, pues no opera como patente de corso frente a derechos fundamentales. La propia ley crea un estatuto reforzado para NNA al reconocer derechos y salvaguardas especiales.

El artículo 21 ocupa un lugar central. Además de las reglas sobre decisiones automatizadas, dispone que los datos sensibles y los datos de NNA no pueden ser tratados salvo que exista autorización expresa del titular o de su representante legal, o que concurra un interés público esencial acompañado de requisitos estrictos de legalidad, proporcionalidad, necesidad y salvaguardas específicas. La misma disposición reconoce que los adolescentes, a partir de los quince años y en ejercicio progresivo de sus derechos, pueden otorgar por sí mismos consentimiento explícito para el tratamiento de sus datos cuando los fines se expliquen con claridad (Asamblea Nacional del Ecuador, 2021, art. 21).

La ley complementa ese régimen con dos mandatos de gran relevancia: reconoce el derecho a la educación digital, entendida como formación para un uso adecua-

do, seguro y responsable de la tecnología, y exige al Estado, a las entidades educativas, a la sociedad civil y a los proveedores de servicios que informen y capaciten sobre el tratamiento responsable de datos de NNA tanto a ellos como a sus representantes legales (Asamblea Nacional del Ecuador, 2021, arts. 23-24). A ello se suma la calificación de los datos de NNA como categoría especial de datos personales (Asamblea Nacional del Ecuador, 2021, art. 25).

Vista en conjunto, la LOPDP no respalda una representación parental incondicionada. Lo que hace es subordinar cualquier decisión sobre datos de NNA a la finalidad protectora de la ley y a principios como licitud, lealtad, transparencia, finalidad, minimización, seguridad y responsabilidad demostrada. Por eso, la intervención del representante legal no opera como una cláusula de inmunidad, sino como un título de actuación limitado por el interés superior y por el propio estatuto reforzado que la norma diseña.

En la Guía de Gestión de Riesgos y Evaluación de Impacto expedida por la SPDP, que concibe la evaluación de impacto como una metodología basada en escenarios de riesgo reales capaces de vulnerar derechos y libertades del titular (SPDP, 2025a). Trasladada al sharenting, la consecuencia es que la publicación de datos de NNA no debe evaluarse solo por la intención afectiva del progenitor, sino por la probabilidad e intensidad de daños previsibles: identificación, exposición a terceros, perfilamiento, daño reputacional, reutilización comercial o tratamiento automatizado.

También debe considerarse la normativa ecuatoriana sobre interés legítimo. La Resolución N.º SPDP-SPD-2025-0041-R exige que esa base de legitimación sea objeto de una evaluación previa, motivada, proporcional y documentada, y no opera como autorización automática frente a datos de NNA (SPDP, 2025d). Por ello, cuando la exposición parental se integra a emprendimientos, marcas personales o campañas privadas, el interés económico o reputacio-

nal del adulto no puede prevalecer sin una ponderación estricta del interés superior y de los derechos del titular menor de edad.

3.4. Reglamento General y la excepción familiar o doméstica

El Reglamento General a la LOPDP, expedido mediante Decreto Ejecutivo No. 904 en 2023, define las actividades familiares o domésticas como aquellas en las que el tratamiento de datos personales se da en un entorno de amistad, parentesco o grupo personal cercano, en propiedad privada, y sin finalidad de comunicación o transferencia con fines comerciales (Presidencia de la República del Ecuador, 2023, art. 4). El elemento decisivo no es, por tanto, la mera relación familiar entre quien publica y quien aparece en el contenido, sino el contexto, el destinatario y la finalidad del tratamiento.

Con este enfoque, una fotografía compartida en un chat privado estrictamente familiar no plantea el mismo problema que una publicación abierta en TikTok, Instagram, YouTube o Facebook; tampoco es equivalente un álbum digital restringido a un círculo reducido de confianza que una narrativa serializada sobre la vida del hijo destinada a construir audiencia, posicionar una marca personal o monetizar contenidos. La excepción doméstica tiene un fundamento claro: evitar que el derecho de datos invada la intimidad genuina de las relaciones personales. Pero pierde sentido cuando el tratamiento sale del ámbito íntimo y entra en la esfera pública, algorítmica o comercial.

3.5. La Norma General SPDP 2026: pérdida del carácter doméstico

La SPDP reforzó esta lectura con la Norma General para el Tratamiento de Datos Personales en Actividades Familiares

o Domésticas. Su artículo 2 establece que la norma es de aplicación obligatoria para los integrantes del sistema de protección de datos personales cuando el tratamiento se efectúe en ese marco (SPDP, 2026a, art. 2). El artículo 3 define difusión pública como la puesta a disposición de un número indeterminado de personas o la accesibilidad

a través de bases de datos de acceso público, redes sociales y plataformas digitales (SPDP, 2026a, art. 3).

La Tabla 1 sistematiza el núcleo normativo de la obligación parental de protección digital y su incidencia sobre el deber parental.

Tabla 1

Núcleo normativo de la obligación parental de protección digital

Primera fase	Segunda fase	Tercera fase
Constitución (arts. 44 y 66 num. 18-21)	Reconoce interés superior, prevalencia de derechos de NNA, protección de imagen, datos personales, intimidad y comunicaciones.	La libertad expresiva parental cede cuando compromete la privacidad, reputación o seguridad del hijo.
CNA (arts. 9, 11, 53 y 60)	Impone responsabilidad compartida de respeto, protección y cuidado; tutela privacidad y exige escuchar la opinión de NNA.	La representación legal no habilita exposición unilateral ilimitada; exige consulta y protección reforzada.
LOPDP (arts. 21-25)	Regula consentimiento progresivo, educación digital, ejercicio de derechos y categoría especial de datos de NNA.	Obliga a tratar datos de NNA bajo salvaguardas reforzadas y restringe decisiones automatizadas y usos intensivos.
Reglamento General (art. 4)	Define actividad familiar o doméstica por entorno íntimo, propiedad privada y ausencia de fines comerciales.	Reduce la excepción doméstica a ámbitos realmente privados y no comercializados.
SPDP 2026 (arts. 4-6)	Ordena evaluar caso por caso, la finalidad, el medio, el alcance y el impacto; la pérdida del carácter doméstico por difusión pública, comercialidad o lesión de derechos.	Somete al régimen ordinario de protección de datos el <i>sharenting</i> público, masivo o monetizado.

Nota: Elaboración propia de la autora a partir de la Constitución de la República del Ecuador, el Código de la Niñez y Adolescencia, la Ley Orgánica de Protección de Datos Personales, su Reglamento General y la Norma General SPDP 2026.

Más importante aún, el artículo 4 dispone que la SPDP evaluará caso por caso si el tratamiento comprende actividades familiares o domésticas, al considerar las circunstancias, la finalidad, el medio utilizado o la extensión de la difusión, mediante una interpretación dinámica atenta a fenómenos tecnológicos, sociales y culturales (SPDP, 2026a, art. 4). El artículo 5 precisa tres criterios para perder el carácter doméstico: i) finalidad comercial; ii) difusión a un número indeterminado de personas; y iii) impacto lesivo en derechos y libertades del titular (SPDP, 2026a, art. 5). Finalmente, el artículo 6 establece que, si se exceden esos límites, continuarán los procedimientos administrativos conforme a la LOPDP, su Reglamento General y la normativa secundaria aplicable (SPDP, 2026a, art. 6).

Para el *sharenting*, el efecto práctico es notable. La autoridad ecuatoriana admite de forma expresa que aquello que se origina en el ámbito familiar puede perder su carácter doméstico cuando circula fuera del círculo de confianza, se abre a audiencias indeterminadas o se inserta en lógicas de marca, publicidad o monetización. Dicho

de otro modo, el origen familiar del contenido no neutraliza el escrutinio de licitud; en ciertos casos, más bien refuerza el estándar de diligencia exigible dada la especial vulnerabilidad del titular.

De forma complementaria, la Norma General ecuatoriana sobre sistemas de inteligencia artificial de 2026 resulta relevante para los riesgos derivados de reutilización algorítmica de imágenes, voz o rasgos biométricos de NNA. La SPDP exige que los responsables y encargados que desarrollen, entrenen, implementen, desplieguen o provean sistemas de IA que traten datos personales de titulares ecuatorianos observen los principios de la LOPDP, informen con claridad sobre el tratamiento automatizado, realicen gestión de riesgos y evaluaciones de impacto, adopten medidas de seguridad, registren tratamientos y se sometan a auditoría (SPDP, 2026b). Aunque la publicación parental no siempre constituya por sí misma desarrollo de IA, incrementa el volumen de insumos que terceros pueden reutilizar para reconocimiento facial, sustitución de identidad, entrenamiento de modelos o generación sintética de contenidos.

4 Estándares internacionales aplicables

La interpretación del derecho ecuatoriano debe armonizarse con los instrumentos internacionales de derechos humanos ratificados por el Estado. En materia de protección de la identidad virtual de NNA, tres referencias son esenciales: la Convención sobre los Derechos del Niño (CDN), la Observación general núm. 25 y la Convención Americana sobre Derechos Humanos (CADH). A ellas se añaden, con valor comparado persuasivo, los desarrollos europeos y latinoamericanos recientes sobre derecho a la imagen, plataformas accesibles a menores, publicidad basada en perfilamiento y

remedios de supresión frente a contenidos publicados por terceros o por familiares.

4.1. Convención sobre los Derechos del Niño

La Convención sobre los Derechos del Niño reconoce, por un lado, el derecho del niño a no ser objeto de injerencias arbitrarias o ilegales en su vida privada, familia, domicilio o correspondencia, ni de ataques ilícitos a su honra y reputación, y a la protección de la ley contra tales interferencias

(Naciones Unidas, 1989, art. 16). Por otro lado, establece que los Estados deben respetar las responsabilidades, derechos y deberes de los padres para proporcionar dirección y orientación de modo consistente con la evolución de las facultades del niño (Naciones Unidas, 1989, art. 5), así como asegurar el derecho del niño a expresar su opinión libremente en todos los asuntos que le afecten, dándole el peso debido según su edad y madurez (Naciones Unidas, 1989, art. 12).

La tensión entre guía parental y privacidad infantil debe resolverse, por tanto, a favor de una parentalidad habilitante y no colonizadora. La CDN no autoriza a los padres a sustituir la subjetividad del hijo en ámbitos donde el propio tratado exige escucha, respeto a la privacidad y protección contra afectaciones reputacionales. En el entorno digital, esto implica que la dirección parental ha de orientarse a educar, proteger y acompañar, no a disponer ilimitadamente de los datos del hijo como recurso narrativo o mercantil.

4.2. Observación general núm. 25: derechos del niño en el entorno digital

La Observación general núm. 25 del Comité de los Derechos del Niño actualiza la CDN para el entorno digital y constituye el estándar interpretativo más relevante sobre la materia. El Comité explica cómo los Estados deben implementar la Convención frente a oportunidades, riesgos y desafíos del entorno digital, a fin de promover, respetar, proteger y cumplir todos los derechos de la niñez en dicho espacio (Comité de los Derechos del Niño, 2021). Su importancia radica en que desplaza cualquier lectura según la cual Internet sería un espacio ajeno o periférico a la protección integral: para el derecho internacional, la vida digital forma parte del ámbito ordinario de vigencia de los derechos del niño.

Aunque la Observación se dirige principalmente a los Estados y a actores empresariales, su lógica alcanza de manera indirecta a la parentalidad. La protección reforzada de privacidad, datos personales y seguridad exige políticas públicas, educación digital, diseño seguro y acceso a remedios; pero también presupone que quienes ejercen cuidados cotidianos actúen de manera compatible con la dignidad y autonomía en desarrollo del niño. Ello incluye evitar la sobreexposición, la recopilación innecesaria de datos, el perfilamiento prematuro y la circulación de contenidos susceptibles de producir daños actuales o futuros.

4.3. Convención Americana sobre Derechos Humanos

La CADH reconoce el derecho al honor y a la dignidad, así como a la protección contra interferencias arbitrarias o abusivas en la vida privada, la vida familiar, el domicilio y la correspondencia, y frente a ataques ilegales al honor o reputación (OEA, 1969, art. 11). Además, establece que todo niño tiene derecho a las medidas de protección requeridas por su condición de menor por parte de su familia, la sociedad y el Estado (OEA, 1969, art. 19), y garantiza recursos judiciales sencillos y efectivos frente a violaciones de derechos fundamentales (OEA, 1969, art. 25).

En clave interamericana, la familia no es solo un espacio de libertad privada, sino también un sujeto obligado a desplegar medidas de protección apropiadas. Cuando la propia familia se convierte en fuente de injerencia abusiva o de exposición desproporcionada, el sistema exige medidas de protección más efectivas. Esto es particularmente importante en casos en que la explotación digital de la imagen del hijo se normaliza bajo narrativas de emprendimiento familiar o creación de contenido, pero produce afectaciones acumulativas a su dignidad e intimidad.

4.4. Estándares europeos orientadores

Si bien no son formalmente vinculantes para Ecuador, ciertos desarrollos europeos son útiles como derecho comparado persuasivo. El Consejo de Europa ha sostenido que los niños tienen derecho a la vida privada y familiar en el entorno digital, incluida la protección de sus datos personales y de la confidencialidad de su correspondencia y comunicaciones privadas, y que padres, cuidadores y educadores deben ser sensibilizados respecto de este derecho (Council of Europe, 2018). Esta línea resulta congruente con la LOPDP ecuatoriana, que impone deberes de educación y capacitación sobre el tratamiento responsable de datos de NNA.

La actualización comparada de los últimos años confirma que la discusión ya no se limita a la privacidad individual, sino que alcanza al diseño de plataformas, la publicidad y el ejercicio de la autoridad parental. En la Unión Europea, el Reglamento de Servicios Digitales exige que las plataformas accesibles a menores adopten medidas apropiadas y proporcionadas para garantizar un alto nivel de privacidad, seguridad y protección, y prohíbe presentar publicidad basada en perfilamiento cuando el destinatario sea menor de edad (Reglamento [UE] 2022/2065, art. 28). Además, las Directrices de la Comisión Europea de 2025 sobre protección de menores en línea precisan medidas frente a *grooming*, contenidos nocivos, comportamientos adictivos, ciberacoso y prácticas comerciales perjudiciales (Comisión Europea, 2025).

Francia ofrece un referente particularmente cercano al problema de la exposición parental. La Ley n.º 2024-120, de 19 de febrero de 2024, incorporó en el Código Civil la regla según la cual los padres protegen en común el derecho a la imagen del hijo menor, deben asociarlo a su ejercicio según edad y madurez y, en caso de desacuerdo o afectación grave, puede intervenir el juez

para restringir la difusión o incluso delegar el ejercicio de ese derecho (República Francesa, 2024). Esta solución comparada refuerza la idea central de este artículo: la representación parental no es titularidad dispositiva, sino poder-deber sujeto a control cuando compromete privacidad, dignidad o integridad moral.

El estándar comparado de diseño adecuado a la edad del Reino Unido es especialmente útil para traducir el interés superior en medidas operativas. El Children's Code del Information Commissioner's Office exige alta privacidad por defecto, minimización de datos, geolocalización desactivada por defecto, límites al perfilamiento, prohibición de técnicas persuasivas que conduzcan a revelar datos innecesarios y mecanismos accesibles para ejercer derechos (Information Commissioner's Office, 2021). Estas reglas no vinculan a Ecuador, pero ofrecen criterios funcionales para evaluar la diligencia parental y la responsabilidad de plataformas en contenidos donde aparecen NNA.

En la misma línea, el Proyecto de Ley Orgánica español para la protección de personas menores de edad en entornos digitales muestra una tendencia comparada hacia el reconocimiento expreso de derechos de NNA a seguridad, privacidad, honor, intimidad, propia imagen y protección de datos en el ecosistema digital (Congreso de los Diputados, 2025). Su utilidad para Ecuador es persuasiva: confirma que la protección de la identidad digital infantil se está desplazando desde la autorregulación familiar hacia estándares jurídicos de prevención, diseño seguro y tutela reforzada.

4.5. Diálogo latinoamericano y aporte específico al caso ecuatoriano

En América Latina, el debate ha avanzado desde la denuncia de riesgos hacia la construcción de deberes familiares y reme-

dios jurídicos. Ordóñez Pineda y Calva Jiménez (2020) desarrollan la noción de corresponsabilidad digital familiar para prevenir amenazas a la privacidad e identidad de menores; Chilano et al. (2023) muestran, desde Argentina, que la práctica del *sharenting* compromete intimidad, identidad digital y derechos personalísimos de las infancias; y Molina Luna (2025) analiza el derecho al olvido frente al *sharenting* y al *oversharenting* como remedio útil, aunque insuficiente, para recuperar cierto control sobre la huella digital. En Colombia, la Sentencia T-245A/22 de la Corte Constitucional constituye un precedente regional relevante al imponer límites a la exposición digital de

menores, dando prevalencia a su imagen, intimidad e interés superior.

Este diálogo regional permite precisar el aporte del presente estudio: no se limita a reiterar los riesgos del *sharenting* ni a importar respuestas europeas, sino que formula una consecuencia dogmática para Ecuador. La combinación entre interés superior, autonomía progresiva, categoría especial de datos de NNA y pérdida de la excepción doméstica por difusión pública, comercialidad o lesión de derechos permite construir una obligación parental de protección digital exigible tanto antes de publicar como después, cuando corresponde retirar, limitar o reparar contenidos.

5 Riesgos jurídicos de la exposición digital parental

La exposición digital parental produce riesgos jurídicos que no son meramente hipotéticos. Lo que está en juego no es solo la comodidad subjetiva del adulto o la preferencia estética respecto de una publicación, sino la configuración temprana de una biografía digital capaz de afectar seguridad, reputación, privacidad y autonomía futura de la persona menor de edad.

5.1. Huella digital no consentida y permanencia

El primer riesgo es la creación de una huella digital no consentida y difícilmente reversible. A diferencia de la memoria familiar analógica, los entornos digitales multiplican la capacidad de copia, indexación, archivo, recombinación y búsqueda. Un contenido retirado de la cuenta originaria puede haber sido descargado, reenviado, capturado o replicado en terceros sitios. En

consecuencia, decisiones parentales tomadas en la primera infancia pueden proyectarse hasta la adolescencia o la adultez temprana, y condicionar oportunidades educativas, laborales y relacionales. Steinberg (2017) advirtió tempranamente que la masificación del *sharenting* produce expedientes digitales de larga duración antes de que el propio niño pueda comprender o consentir sus efectos.

La permanencia adquiere mayor gravedad cuando se observa que las autoridades europeas de protección de datos han empezado a tratar el *sharenting* como fuente autónoma de riesgos. La Agencia Española de Protección de Datos (AEPD) advierte que las imágenes pueden descargarse, manipularse, reutilizarse con fines publicitarios o escapar definitivamente del control del adulto que las publicó; la Data Protection Commission irlandesa (DPC), en su campaña *Pause Before You Post*, enfatiza que la huella digital creada tempranamente puede ser difícil de borrar y que mu-

chas publicaciones revelan nombre, edad, rutinas, amistades o ubicación (Agencia Española de Protección de Datos, 2024; Data Protection Commission, 2025). Estos criterios refuerzan el deber de temporalidad: revisar, retirar o restringir contenidos cuando dejan de ser necesarios.

5.2. Afectación de privacidad, honor e imagen

El segundo riesgo es la lesión directa a derechos personalísimos. El *sharenting* puede revelar información sobre salud, conducta, castigos, dificultades emocionales, desnudez parcial, crisis familiares o situaciones escolarmente sensibles. Este tipo de contenidos incide de forma inmediata en la dignidad, la imagen y el honor de NNA, y puede comprometer la intimidad de la vida privada y familiar. No toda publicación infantil es lesiva, pero la evaluación debe realizarse desde la perspectiva del titular, no del placer expresivo del adulto. La investigación de Sarkadi et al. (2020) mostró que niñas, niños y adolescentes quieren ser consultados antes de que sus padres publiquen contenidos sobre ellos. De modo similar, Ouvrein y Verswijvel (2019) identifican tensiones entre la autoimagen que adolescentes desean proyectar y la imagen digital previamente construida por sus padres.

5.3. Seguridad física y riesgos de victimización

El tercer riesgo concierne a la seguridad. Fotografías en uniformes, placas de vehículos, nombres de centros educativos, geolocalización automática, rutinas horarias o interior del domicilio pueden facilitar procesos de identificación por terceros, incluidos agresores sexuales, acosadores, extorsionadores o estafadores. La lesión

no depende de que el progenitor obre con intención dañosa; basta con que la publicación reduzca indebidamente la esfera de reserva y aumente la vulnerabilidad del titular. En niños pequeños, además, la imposibilidad práctica de comprender los alcances del entorno digital exige un estándar de precaución más alto.

La seguridad física y digital se dificulta por la posibilidad de inferir datos no explícitos a partir de imágenes ordinarias. La AEPD identifica como riesgos la geolocalización, el *grooming*, el ciberacoso y el uso de contenidos con propósitos sexuales; la Commission Nationale de l'Informatique et des Libertés (CNIL), por su parte, reconoce que imágenes publicadas por familiares pueden terminar en redes de explotación o ser objeto de solicitudes de retirada por los propios niños afectados (Agencia Española de Protección de Datos, 2024; Commission Nationale de l'Informatique et des Libertés, 2025). En consecuencia, el análisis jurídico debe considerar no solo el dato visible, sino también metadatos, contexto, audiencia y posibilidad de captura o redistribución.

5.4. Perfilamiento, dataficción y decisiones automatizadas

El cuarto riesgo proviene de la dataficción. Cada imagen, comentario o interacción puede alimentar sistemas de recomendación, publicidad comportamental, reconocimiento facial o inferencias sobre preferencias, nivel socioeconómico, entorno familiar, estado de salud y personalidad. La LOPDP prohíbe para NNA determinados tratamientos automatizados sin bases y salvaguardas reforzadas, precisamente porque el perfilamiento puede afectar derechos y libertades fundamentales (Asamblea Nacional del Ecuador, 2021, art. 21). La construcción de identidades digitales prematuras por parte de los propios padres incrementa el volumen de datos que terceros pueden

reutilizar con fines comerciales o discriminatorios.

Este riesgo ha cambiado cualitativamente con la IA generativa. UNICRI advierte que la IA puede facilitar nuevas formas de explotación sexual infantil en línea mediante la creación, modificación o escalamiento de material abusivo; WeProtect Global Alliance identifica, para el periodo 2023-2025, una evolución de la explotación sexual infantil facilitada por tecnología que exige prevención y responsabilidades de diseño (UNICRI, 2024; WeProtect Global Alliance, 2025). Para el *sharenting*, esto supone que cada imagen identificable de un NNA puede convertirse en insumo para sustitución de rostro, clonación de voz, *deepfakes* o simulaciones dañinas, aunque la publicación originaria haya sido afectiva o aparentemente inocua.

5.5. Mercantilización afectiva y family influencing

Un quinto riesgo, especialmente actual, es la mercantilización afectiva. Bajo el modelo del *family influencing*, la cotidianeidad del hogar se convierte en materia prima de audiencias, patrocinios, campañas o monetización por visualizaciones. La imagen y vida de NNA pasa a integrarse en estrategias de posicionamiento de marca personal o emprendimiento familiar. Jurídicamente, este fenómeno agrava la ilicitud potencial por dos razones. La primera es que el fin comercial hace perder, por definición, el carácter familiar o doméstico del tratamiento conforme al Reglamento y a la Norma SPDP 2026 (Presidencia de la República del Ecuador, 2023, art. 4; SPDP, 2026a, art. 5.1). La segunda es que la exposición deja de ser accesoria para convertirse en estructural al negocio, con incentivos para intensificar publicaciones, dramatizar intimidades o ignorar objeciones del propio NNA.

Sobre influencers familiares la mercantilización no siempre adopta la forma de publicidad explícita. Ågren (2023) muestra cómo los niños pueden funcionar como capital digital en cuentas de influencers, al integrarse en narrativas que fortalecen marcas parentales; Baxter y Czarnecka (2025), mediante análisis de 5.253 publicaciones de *influencers* de maternidad británicas, evidencian una paradoja de privacidad: las creadoras pueden afirmar preocupación por sus hijos mientras los exponen de manera sostenida; y Lockett (2025) propone diferenciar el *sharenting* ordinario de la actuación de *family influencers*, precisamente porque esta última estructura la presencia infantil como componente del negocio. Este enfoque es útil para Ecuador porque permite calificar como comercial o cuasicomercial la exposición repetida que aumenta audiencia, reputación o tráfico económico, aunque no haya patrocinio individual identificado.

5.6. Conflictos familiares y autonomía progresiva

Finalmente, la exposición digital puede deteriorar el vínculo familiar. Blum-Ross y Livingstone (2017) observaron que el *sharenting* se ubica en una frontera compleja entre apoyo comunitario, autoexpresión parental y delimitación del yo digital del hijo. Cuando la publicación se vuelve unilateral y repetitiva, emerge una forma de colonización narrativa: la vida del niño es relatada por otro antes de que pueda auto-representarse. Ello entra en fricción con la autonomía progresiva, con el derecho a ser consultado y con la necesidad de que la identidad digital futura sea construida también desde la voluntad del propio titular.

6 Contenido de la obligatoriedad parental en la protección de la identidad virtual

Del bloque normativo examinado no emerge una simple recomendación ética, sino un conjunto de deberes jurídicos concretos. En Ecuador, la protección de la identidad virtual de NNA impone a madres, padres y representantes deberes de abstención, prudencia, consulta, seguridad y corrección.

6.1. Deber de abstención frente a exposiciones innecesarias

El primero de esos deberes consiste en no exponer innecesariamente. Madres, padres y representantes deben abstenerse de publicar, comunicar o conservar de manera excesiva datos personales de NNA cuando la exposición no responda a una finalidad legítima vinculada con cuidado o protección. La lógica de minimización impide normalizar publicaciones sobre salud, escolaridad, conflictos conductuales, corporalidad, castigos o crisis emocionales sin una justificación particularmente intensa, pues se trata de información sensible o potencialmente lesiva para la reputación futura del titular.

6.2. Deber de finalidad legítima y minimización

Cuando exista una razón atendible para comunicar cierta información, por ejemplo, activar una red privada de apoyo frente a un problema concreto, el tratamiento debe seguir siendo estrictamente limitado. La pregunta jurídica relevante no es si el adulto desea compartir, sino qué cantidad de datos, por cuánto tiempo, ante

qué audiencia y con qué grado de identificación resulta realmente necesaria. Desde esa perspectiva, anonimizar, seudonimizar, cerrar audiencias o suprimir geolocalización no son gestos de prudencia opcional, sino manifestaciones prácticas del deber de minimización.

6.3. Deber de escucha y participación progresiva

También existe un deber de escucha y participación progresiva. El CNA y la CDN reconocen que NNA deben ser consultados en los asuntos que les afecten y que su opinión debe ponderarse conforme a su edad y madurez (Congreso Nacional del Ecuador, 2003, art. 60; Naciones Unidas, 1989, art. 12). La LOPDP refuerza ese diseño al permitir que adolescentes desde los quince años consientan explícitamente el tratamiento de sus datos personales y ejerzan derechos directamente ante la Autoridad o el responsable del tratamiento (Asamblea Nacional del Ecuador, 2021, arts. 21 y 24). De ahí que, a mayor edad y madurez, menor sea el espacio para decisiones unilaterales de exposición parental. Incluso antes de los quince años, la consulta sigue siendo exigible como expresión del interés superior y de la autonomía progresiva.

6.4. Deber de seguridad y privacidad por defecto

A lo anterior se suma un deber de seguridad y privacidad por defecto. Quien decide tratar datos de sus hijos en entornos digitales debe configurar niveles altos de

privacidad, restringir audiencias, desactivar geolocalización, evitar metadatos innecesarios, revisar periódicamente la permanencia del contenido y suprimir lo que haya perdido justificación. En la era digital, la crianza diligente incluye alfabetización tecnológica y jurídica básica, priorizando su bienestar y protección integral.

En términos de deber parental, la privacidad por defecto exige escoger siempre la configuración menos invasiva posible antes de publicar: cuenta privada, audiencia limitada, ausencia de geolocalización, supresión de metadatos, pixelado o no exhibición del rostro, omisión de uniformes y eliminación periódica. La Guía ecuatoriana de protección de datos desde el diseño y por defecto señala que los tratamientos deben anticipar riesgos futuros y que, por defecto, solo deben tratarse los datos necesarios para cada finalidad; el Children's Code coincide en exigir alta privacidad, minimización y geolocalización desactivada por defecto cuando se trata de menores (SPDP, 2025b; Information Commissioner's Office, 2021).

6.5. Deber de no mercantilización sin salvaguardas reforzadas

Especial cautela merece la explotación económica de la imagen, voz o rutina de NNA. Cuando el contenido se integra a patrocinios, monetización, campañas o estrategias estables de construcción de audiencia, la justificación debe ser extraordinariamente estricta. En estos escenarios no basta invocar el consentimiento parental: el fin comercial desplaza la excepción doméstica y evidencia un conflicto de interés entre el beneficio reputacional o económico del adulto y los riesgos presentes y futuros que asume el NNA. La representación legal no puede utilizarse para validar ese desequilibrio.

6.6. Deber de corrección, supresión y reparación

Por último, el deber de protección incluye corregir, restringir o suprimir cuando la publicación ya no sea necesaria, cuando surja un riesgo no previsto o cuando el propio NNA formule una objeción razonable. La intensidad de esta obligación crece con la edad y la capacidad de autodeterminación del titular. La permanencia obstinada de contenidos lesivos puede constituir una vulneración continuada de derechos y abrir paso a medidas de cese, supresión, tutela administrativa ante la SPDP, acciones judiciales y eventuales reclamaciones civiles por daños.

La supresión no debe entenderse únicamente como borrar una publicación de la cuenta originaria. La regulación ecuatoriana sobre seudonimización, anonimización, bloqueo y eliminación exige considerar el ciclo de vida del dato y las medidas técnicas para impedir identificación o reidentificación sin esfuerzos desproporcionados (SPDP, 2025c). En publicaciones parentales, esto se traduce en retirar contenido, solicitar eliminación a plataformas, bloquear accesos, anonimizar descripciones, eliminar etiquetas y pedir a terceros que cesen la retransmisión, especialmente cuando el NNA objeta o cuando aparece un riesgo no previsto.

7 Test de juridicidad para publicaciones parentales sobre niños, niñas y adolescentes (NNA)

A efectos de operativizar la obligatoriedad parental propuesta, conviene formular un test de juridicidad aplicable antes de publicar o difundir datos de NNA. Este test no sustituye el análisis caso por caso, pero sí traduce el marco normativo en preguntas de decisión práctica.

a) Finalidad: ¿La publicación responde a una necesidad legítima de cuidado, protección o comunicación íntima, o persigue visibilidad, entretenimiento adulto o monetización?

b) Necesidad: ¿La finalidad puede alcanzarse sin publicar el dato o usando un medio menos intrusivo?

c) Minimización: ¿Se limita el contenido a los datos estrictamente indispensables? ¿Puede omitirse rostro, nombre, ubicación, uniforme, centro educativo o información de salud?

d) Audiencia: ¿El contenido queda restringido a un círculo reducido de confianza o es accesible a un número indeterminado de personas?

e) Consulta: ¿Se escuchó al NNA de acuerdo con su edad y madurez? ¿Existe objeción expresa o razonablemente previsible?

f) Impacto: ¿La publicación puede generar vergüenza, estigmatización, riesgo de acoso, exposición sexualizada, perfilamiento o daño reputacional futuro?

g) Temporalidad: ¿Es necesario conservar el contenido en línea? ¿Se prevé su revisión o eliminación posterior?

h) Comercialidad: ¿Existe patrocinio, monetización, publicidad o beneficio reputacional estructural asociado al contenido?

i) Responsabilidad: ¿El adulto puede justificar ex post, con razones objetivas, que la decisión fue compatible con el interés superior, la autonomía progresiva y la protección de datos?

A este test conviene añadir dos verificaciones operativas. Primero, una verificación de diseño y configuración: ¿la publicación se hizo con privacidad alta, sin geolocalización, sin metadatos, sin rostro identificable cuando no era imprescindible y sin información escolar o sanitaria? Segundo, una verificación de riesgo residual: ¿qué daño subsiste, aunque la publicación sea restringida y qué medidas existen para retirar, anonimizar o bloquear el contenido? Estos filtros conectan el test con la gestión de riesgos y evaluación de impacto de la SPDP, con el enfoque de privacidad por defecto y con los estándares europeos de plataformas accesibles a menores (SPDP, 2025a; SPDP, 2025b; Comisión Europea, 2025; Information Commissioner's Office, 2021).

Cuando una o varias respuestas revelen finalidad comercial, difusión pública indiscriminada, ausencia de consulta o impacto relevante sobre privacidad, honor, seguridad o reputación, la regla debe ser la no publicación. En el ámbito judicial o administrativo, además, permite valorar diligencia, previsibilidad del daño y eventual abuso de la representación parental. Su utilidad práctica consiste en trasladar la discusión desde una autorización genérica de los padres hacia una carga argumentativa: quien decide publicar debe poder explicar por qué la medida era legítima, necesaria, mínima, segura y respetuosa de la autonomía progresiva.

8 Discusión

La objeción más fuerte a la tesis de este trabajo se apoya en la autonomía familiar y en la libertad de expresión de madres y padres. No se trata de un reparo superficial. La vida familiar se construye también mediante relatos, fotografías, memorias compartidas y redes de apoyo; un derecho demasiado invasivo podría desplazar indebidamente al Estado hacia zonas de intimidad genuina. Sin embargo, ese riesgo no obliga a aceptar una inmunidad general para toda exposición de NNA. El punto decisivo es distinguir entre memoria o comunicación íntima y difusión pública o comercial de datos personales. El derecho de datos no pretende vigilar la crianza cotidiana; interviene cuando la publicación sale del círculo de confianza o cuando afecta derechos fundamentales del hijo.

Tampoco resulta suficiente sostener que la voluntad parental coincide siempre con el interés del NNA. El derecho de familia contemporáneo justamente parte de la premisa contraria: la representación existe porque puede haber tensiones, errores de apreciación o conflictos de interés y, por ello, se la rodea de principios, límites y remedios. En materia digital, esas tensiones se intensifican por la persistencia del contenido, la economía de plataformas y el valor reputacional o económico que ciertas exposiciones generan para el adulto. La LOPDP, el CNA y la CDN cumplen aquí una función correctiva: reconducen el ejercicio de la parentalidad hacia fines de protección y no de apropiación narrativa o comercial.

Desde luego, el marco ecuatoriano todavía deja preguntas abiertas. Persisten zonas grises sobre monetización indirecta, deberes específicos de las plataformas ante solicitudes formuladas por adolescentes, tratamiento en grupos familiares híbridos y criterios para cuantificar el daño reputacional digital. Aun así, el núcleo normativo vi-

gente permite afirmar que el *sharenting* no constituye un espacio ajeno al derecho. La mayor aportación de la regulación de 2026 no radica en crear el problema, sino en cerrar una defensa frecuente: la idea de que toda publicación realizada por familiares queda automáticamente fuera del derecho de protección de datos.

La monetización indirecta merece desarrollo específico porque no siempre aparece como patrocinio explícito o pago por publicación. También existe cuando la exposición constante del hijo incrementa seguidores, interacción, reputación, tráfico hacia emprendimientos, invitaciones comerciales o valor de marca personal del adulto. En tales supuestos, aunque no haya contrato publicitario individual, la imagen del NNA opera como insumo económico de una estrategia de visibilidad. Por ello, el análisis no debe limitarse a preguntar si hubo ingreso directo, sino si la publicación integra una actividad sistemática orientada a audiencia, posicionamiento o beneficio patrimonial indirecto. Si la respuesta es afirmativa, la excepción doméstica se debilita y el estándar de licitud debe aproximarse al de un responsable de tratamiento, con exigencias de finalidad determinada, minimización, proporcionalidad, seguridad, documentación de la decisión y mecanismos expeditos de retiro.

En adelante, sería conveniente que la SPDP emita directrices más detalladas sobre tratamiento de datos de NNA por representantes legales y sobre actividad de *family influencing*, con ejemplos de prácticas incompatibles con la LOPDP, parámetros reforzados de diligencia y mecanismos expeditos de supresión. También sería deseable una coordinación más visible entre la SPDP, el sistema de protección integral de niñez y adolescencia, las autoridades educativas y las plataformas digitales, de modo que la

educación digital prevista por la ley se traduzca en pautas concretas para familias, docentes y adolescentes.

Finalmente, las investigaciones futuras deberían incorporar el contexto educativo. UNICEF (2024) advierte que los sistemas escolares procesan grandes volúmenes de datos personales y requieren obligaciones claras de gobernanza, seguridad y privacidad, por lo que la exposición de NNA no

solo ocurre en redes parentales, sino también mediante publicaciones institucionales, plataformas educativas, fotografías escolares y herramientas EdTech. En Ecuador, ello justifica articular la SPDP, el sistema de protección integral de niñez y adolescencia y las instituciones educativas para definir criterios específicos sobre imágenes, uniformes, eventos escolares, consentimiento, oposición adolescente y supresión.

9 Conclusiones

La lectura conjunta de la Constitución, el CNA, la LOPDP, su Reglamento General y la normativa secundaria de la SPDP permite sostener una conclusión nítida: en Ecuador, la parentalidad digital está jurídicamente configurada como deber de protección y no como facultad irrestricta de exposición. No hace falta crear una categoría autónoma para llegar a ese resultado; basta con articular coherentemente los derechos de intimidad, imagen, honra, autodeterminación informativa e interés superior de NNA.

Ese deber se traduce, en términos concretos, en limitar exposiciones innecesarias, minimizar datos, escuchar de forma progresiva, adoptar medidas de privacidad y seguridad, evitar la mercantilización de la vida del hijo y corregir o suprimir contenidos cuando exista objeción o riesgo. La función parental no desaparece por reconocer estos límites; se redefine conforme a un estándar de acompañamiento diligente y respetuoso de la dignidad del NNA.

En consecuencia, la excepción familiar o doméstica no puede ser utilizada para acoger la difusión pública, uso comercial o tratamientos que lesionen derechos y libertades de NNA. Con la norma general de 2026, el derecho ecuatoriano ha precisado que lo doméstico deja de serlo cuando los datos salen del círculo íntimo o se insertan

en lógicas de audiencia y monetización. En tales supuestos, la actuación parental queda sometida plenamente a la LOPDP y puede generar consecuencias administrativas, judiciales y reparadoras.

La fórmula final es sencilla, aunque sus efectos sean exigentes: quien ejerce el cuidado de NNA tiene el deber jurídico de no hipotecar anticipadamente la identidad digital futura de sus hijos. Proteger esa identidad no significa desconfiar de la familia, sino actualizar la responsabilidad parental frente a una sociedad atravesada por plataformas, datos persistentes y memorias difíciles de borrar.

La actualización normativa y comparada confirma que el estándar de diligencia debe integrar cuatro dimensiones: i) gestión previa de riesgos; ii) privacidad por defecto; iii) prevención frente a IA generativa y reutilización maliciosa; y iv) control reforzado de monetización directa o indirecta. En consecuencia, la juridicidad de la exposición parental depende menos del vínculo familiar y más del alcance, finalidad, destinatarios, reversibilidad y capacidad real de demostrar que la decisión fue compatible con el interés superior del NNA.

Como limitación, este estudio no incorpora entrevistas, análisis de cuentas de redes sociales ni medición empírica de

prácticas parentales en Ecuador; su alcance es dogmático, normativo y comparado. Por ello, futuras investigaciones se deberían examinar, con métodos empíricos y enfoque regional andino, cómo madres, padres,

adolescentes, plataformas y autoridades comprenden la excepción doméstica, la monetización indirecta y los mecanismos de supresión o reparación frente a contenidos publicados por familiares.

Fuentes de financiamiento

Este trabajo no recibió financiamiento específico de agencias del sector público, sector comercial o entidades sin fines de lucro.

Conflicto de intereses

Los autores declaran que no existen conflictos de intereses.

Referencias

- Agencia de Acceso a la Información Pública. (2024, 16 de agosto). Protección de datos y privacidad de niños, niñas y adolescentes en entornos digitales. <https://www.argentina.gob.ar/noticias/proteccion-de-datos-y-privacidad-de-ninos-ninas-y-adolescentes-en-entornos-digitales>
- Agencia Española de Protección de Datos. (2024, 28 de junio). Los riesgos del sharenting en la vida de los menores. <https://www.aepd.es/prensa-y-comunicacion/blog/los-riesgos-del-sharenting-en-la-vida-de-los-menores>
- Ågren, Y. (2023). Branded childhood: Infants as digital capital on Instagram. *Childhood*, 30(1), 9-23. <https://doi.org/10.1177/09075682221129367>
- Ammerman Yebra, J. (2018). El régimen de prestación del consentimiento para la intromisión en los derechos de la personalidad de los menores. Especial referencia al fenómeno del *sharenting*. *Actualidad Jurídica Iberoamericana*, 8(extra), 253-264.
- Amon, M. J., Kartvelishvili, N., Bertenthal, B. I., Hugenberg, K., & Kapadia, A. (2022). Sharenting and children's privacy in the United States: Parenting style, practices, and perspectives on sharing young children's photos on social media. *Proceedings of the ACM on Human-Computer*

- Interaction, 6(CSCW1), Article 116. <https://doi.org/10.1145/3512963>
- Asamblea Nacional del Ecuador. (2021, 26 de mayo). Ley Orgánica de Protección de Datos Personales. Registro Oficial, Quinto Suplemento No. 459. <https://www.asambleanacional.gob.ec/es/multi-medios-legislativos/63464-ley-organica-de-proteccion-de-datos>
- Azurmendi, A., Etayo, C., & Torrell, A. (2021). *Sharenting* y derechos digitales de los niños y adolescentes. Profesional de la información, 30(4), e300407. <https://doi.org/10.3145/epi.2021.jul.07>
- Barba, V. (2025). Derecho a la identidad digital y protección de niños, niñas y adolescentes frente a la exposición prematura en redes. Revista de Ciencias Sociales, 87. <https://doi.org/10.22370/rcs.2025.87.5008>
- Baxter, K., & Czarnecka, B. (2025). Sharing images of children on social media: British motherhood influencers and the privacy paradox. PLOS ONE, 20(1), e0314472. <https://doi.org/10.1371/journal.pone.0314472>
- Berg, V., Arabiat, D., Morelius, E., Kervin, L., Zgambo, M., Robinson, S., Jenkins, M., & Whitehead, L. (2024). Young children and the creation of a digital identity on social networking sites: Scoping review. JMIR Pediatrics and Parenting, 7, e54414. <https://doi.org/10.2196/54414>
- Blum-Ross, A., & Livingstone, S. (2017). *Sharenting*, parent blogging, and the boundaries of the digital self. Popular Communication, 15(2), 110-125. <https://doi.org/10.1080/15405702.2016.1223300>
- Cataldo, I., Lieu, A. A., Carollo, A., Bornstein, M. H., Gabrieli, G., Lee, A., & Esposito, G. (2022). From the cradle to the web: The growth of “sharenting”—A scientometric perspective. Human Behavior and Emerging Technologies, 2022, Article 5607422. <https://doi.org/10.1155/2022/5607422>
- Cebrián Beltrán, S. (2023). *Sharenting*: nuevo reto para el derecho a la imagen y a la protección de datos de la infancia y la adolescencia. Lex Social: Revista de Derechos Sociales, 13(2), 1-21. <https://doi.org/10.46661/lexsocial.8227>
- Chilano, M. B., Tarullo, R., & Frezzotti, Y. (2023). La práctica del *sharenting*: Implicancias en la intimidad e identidad digital de las infancias. La Trama de la Comunicación, 27(1), 068-089. <https://doi.org/10.35305/lt.v27i1.823>
- Comisión Europea. (2025). Directrices sobre medidas para garantizar un elevado nivel de privacidad, seguridad y protección de los menores en línea, de conformidad con el artículo 28, apartado 4, del Reglamento (UE) 2022/2065. Diario Oficial de la Unión Europea, C/2025/5519. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:C_202505519
- Commission Nationale de l'Informatique et des Libertés. (2025, 28 de noviembre). Sharing photos and videos of your child on social networks: What risks. <https://www.cnil.fr/en/sharing-photos-and-videos-your-child-social-networks-what-risks>
- Comité de los Derechos del Niño. (2021). Observación general núm. 25 (2021) relativa a los derechos de los niños en relación con el entorno digital. Naciones Unidas. <https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation>
- Congreso de los Diputados. (2025, 11 de abril). Proyecto de Ley Orgánica para la

- protección de las personas menores de edad en los entornos digitales (BOCG, Serie A, Núm. 52-1). https://www.congreso.es/public_oficiales/L15/CONG/BOCG/A/BOCG-15-A-52-1.PDF
- Congreso Nacional del Ecuador. (2003, 3 de enero). Código de la Niñez y Adolescencia. Registro Oficial No. 737.
- Constitución de la República del Ecuador. (2008, 20 de octubre). Registro Oficial No. 449.
- Corte Constitucional de Colombia. (2022). Sentencia T-245A/22. <https://www.corteconstitucional.gov.co/Relatoria/2022/T-245A-22>
- Council of Europe. (2018). Guidelines to respect, protect and fulfil the rights of the child in the digital environment. <https://rm.coe.int/guidelines-to-respect-protect-and-fulfil-the-rights-of-the-child-in-th/16808d881a>
- Data Protection Commission. (2025). Children: "Pause Before You Post" awareness campaign. <https://dataprotection.ie/en/children>
- Ferrara, P., Cammisa, I., Zona, M., Cimaroli, E., Sacco, R., Pacucci, I., Grimaldi, M. T., Scaltrito, F., Pettoello-Mantovani, M., & Corseillo, G. (2024). The awareness of sharenting in Italy: A pilot study. *Italian Journal of Pediatrics*, 50, Article 226. <https://doi.org/10.1186/s13052-024-01797-5>
- Hinojo-Lucena, F. J., Aznar-Díaz, I., Cáceres-Reche, M. P., Trujillo-Torres, J. M., & Romero-Rodríguez, J. M. (2020). *Sharenting*: Internet addiction, self-control and online photos of underage children. *Comunicar*, 64, 97-108. <https://doi.org/10.3916/C64-2020-09>
- Information Commissioner's Office. (2021). Age appropriate design: A code of practice for online services. <https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/>
- Livingstone, S., & Third, A. (2017). Children and young people's rights in the digital age: An emerging agenda. *New Media & Society*, 19(5), 657-670. <https://doi.org/10.1177/1461444816686318>
- Lockett, T. (2025). Smile for the camera: Balancing parental rights and children's privacy in the age of family influencers. *Northwestern University Law Review Online*, 119, 355. <https://northwesternlawreview.org/articles/smile-for-the-camera-balancing-parental-rights-and-childrens-privacy-in-the-age-of-family-influencers/>
- Molina Luna, M. (2025). La privacidad y protección de datos de los menores de edad en la era de la tecnología disruptiva: El derecho al olvido, el *sharenting* y el *oversharenting*. *Pro Jure Revista de Derecho*, 64. <https://doi.org/10.4151/SO2810-76592025064-1435>
- Naciones Unidas. (1989, 20 de noviembre). Convención sobre los Derechos del Niño. <https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child>
- OCDE. (2025). Children in the digital environment: Revised typology of risks. OECD Publishing. https://www.oecd.org/en/publications/children-in-the-digital-environment_9b8f222e-en.html
- Ordóñez Pineda, L., & Calva Jiménez, S. (2020). Amenazas a la privacidad de los menores de edad a partir del *sharenting*. *Revista Chilena de Derecho y*

- Tecnología, 9(2), 105-130. <https://doi.org/10.5354/0719-2584.2020.55333>
- Organización de los Estados Americanos. (1969, 22 de noviembre). Convención Americana sobre Derechos Humanos. <https://www.oas.org/en/iachr/mandate/basics/american-convention-on-human-rights.asp>
- Ouvrein, G., & Verswijvel, K. (2019). *Sharenting*: Parental adoration or public humiliation? A focus group study on adolescents' experiences with *sharenting* against the background of their own impression management. *Children and Youth Services Review*, 99, 319-327. <https://doi.org/10.1016/j.childyouth.2019.02.011>
- Presidencia de la República del Ecuador. (2023, 13 de noviembre). Decreto Ejecutivo No. 904. Reglamento General a la Ley Orgánica de Protección de Datos Personales. Registro Oficial, Tercer Suplemento No. 435. <https://www.registroficial.gob.ec/tercer-suplemento-al-registro-oficial-no-435/>
- Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, de 19 de octubre de 2022, relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales). *Diario Oficial de la Unión Europea*, L 277, 1-102.
- República Francesa. (2024). Loi n° 2024-120 du 19 février 2024 visant à garantir le respect du droit à l'image des enfants. *Journal officiel de la République française*. <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000049163317>
- Sarkadi, A., Dahlberg, A., Fängström, K., & Warner, G. (2020). Children want parents to ask for permission before *sharenting*. *Journal of Paediatrics and Child Health*, 56(6), 981-983. <https://doi.org/10.1111/jpc.14945>
- Steinberg, S. B. (2017). *Sharenting*: Children's privacy in the age of social media. *Emory Law Journal*, 66(4), 839-884. <https://scholarlycommons.law.emory.edu/elj/vol66/iss4/2/>
- Superintendencia de Protección de Datos Personales. (2025a). Resolución N.º SPDP-SPD-2025-0003-R: Guía de gestión de riesgos y evaluación de impacto del tratamiento de datos personales. <https://spdp.gob.ec/resolucion-n-sdpd-spd-2025-0003-r-guia-de-gestion-de-riesgos-y-evaluacion-de-impacto-del-tratamiento-de-datos-personales-con-su-anexo/>
- Superintendencia de Protección de Datos Personales. (2025b). Guía de protección de datos personales desde el diseño y por defecto. <https://spdp.gob.ec/guias-sdpd/>
- Superintendencia de Protección de Datos Personales. (2025c). Resolución N.º SPDP-SPD-2025-0030-R: Reglamento para la seudonimización, anonimización, bloqueo y eliminación de datos personales. <https://spdp.gob.ec/resol/>
- Superintendencia de Protección de Datos Personales. (2025d). Resolución N.º SPDP-SPD-2025-0041-R: Normativa general para la aplicación del interés legítimo como base de legitimación para el tratamiento de datos personales dentro del territorio de la República del Ecuador. https://spdp.gob.ec/resolucion_041/
- Superintendencia de Protección de Datos Personales. (2026a). Resolución No. SPDP-SPD-2026-0003-R: Norma general para el tratamiento de datos personales en actividades familiares o domésticas. <https://spdp.gob.ec/resolucion-3/>

- Superintendencia de Protección de Datos Personales. (2026b). Resolución N.º SPDP-SPD-2026-0009-R: Norma general para la garantía del derecho de protección de datos personales en el uso de sistemas de inteligencia artificial. https://spdp.gob.ec/resoluciones_spdp/
- Tosuntaş, Ş. B., & Griffiths, M. D. (2024). Sharenting: A systematic review of the empirical literature. *Journal of Family Theory & Review*, 16(3), 525-562. <https://doi.org/10.1111/jftr.12566>
- UNICEF. (2024). Data protection in schools: Guidance for legislators, policy makers and education institutions. <https://www.unicef.org/eca/reports/data-protection-schools>
- UNICRI. (2024). Generative AI: A new threat for online child sexual exploitation and abuse. United Nations Interregional Crime and Justice Research Institute. <https://unicri.org/generative-ai-new-threat-online-child-sexual-exploitation-and-abuse-september-2024>
- WeProtect Global Alliance. (2025). Global Threat Assessment 2025. <https://www.weprotect.org/global-threat-assessment-25/>