

Mijhail Pavel Pardo Lafuente* (Bolivia)

Las características específicas de los entornos en línea pueden generar una falsa sensación de privacidad, intensificar las emociones negativas y aumentar la impulsividad, todo lo cual puede modificar la naturaleza del acoso en línea o intensificar sus consecuencias.

SONIA LIVINGSTONE Y ALICIA BLUM-ROSS, 2020

La privacidad nos protege de presiones no deseadas y abusos de poder. La necesitamos para ser individuos autónomos, y las democracias solo pueden funcionar bien cuando los ciudadanos gozamos de autonomía.

CARISSA VÉLIZ, 2024

¿Infancia bajo vigilancia? Sobre la protección del derecho a la autodeterminación informacional de las personas menores de edad en contextos digitales

RESUMEN

En un contexto de creciente digitalización y consolidación de arquitecturas algorítmicas de poder, este trabajo analiza, desde una perspectiva iusfilosófica y de derechos humanos, la reconfiguración del consentimiento infantil en entornos digitales como una categoría jurídica reforzada. A partir del estudio del *corpus iuris* internacional y de normas modelo con proyección regional, como el Reglamento General de Protección de Datos (RGPD) europeo, se sostiene que el consentimiento de niños, niñas y adolescentes no debe entenderse como una mera formalidad procedimental, sino como una garantía sustantiva. El artículo identifica un déficit normativo en diversos

* Abogado, Universidad Mayor de San Simón; magíster en Derechos Humanos de las Poblaciones Más Vulnerables, Universidad Andina Simón Bolívar; maestrando en Global Rule of Law and Constitutional Democracy, Università degli Studi di Genova. Profesor de Derecho Internacional y Argumentación Jurídica, Universidad del Valle. mpardol@univalle.edu / orcid: [0000-0003-4210-349X](https://orcid.org/0000-0003-4210-349X)

países latinoamericanos, en particular Bolivia, donde el consentimiento infantil se ve debilitado por prácticas estatales y empresariales poco transparentes. Frente a ello, se propone una reconstrucción normativa que incorpore mecanismos de participación efectiva, responsabilidad algorítmica y evaluaciones de impacto en derechos humanos, basadas en principios del Comité de los Derechos del Niño, como la minimización de datos, la transparencia y la proporcionalidad.

Palabras clave: autodeterminación informativa; consentimiento; privacidad; ecosistemas digitales; niños, niñas y adolescentes.

Children Under Surveillance? Regarding Protection of Minors' Right to Informational Self-Determination in Digital Contexts

ABSTRACT

In the context of increasing digitalization and consolidation of algorithmic power architectures, this paper analyzes, from a legal-philosophical and human rights-based perspective, the reconfirmation of children's consent in digital environments as a reinforced legal category. Based on a study of the international *corpus iuris* and model norms with regional scope, such as the European General Data Protection Regulation (GDPR), it argues that the consent of children and adolescents should not be understood as a mere procedural formality, but rather as a substantive guarantee. The article identifies a regulatory deficit in different Latin American countries, especially Bolivia, where child consent is weakened by non-transparent state and corporate practices. In response, it proposes a regulatory overhaul that incorporates mechanisms for effective participation, algorithmic accountability, and human rights impact assessments, based on principles from the Committee on the Rights of the Child, such as data minimization, transparency, and proportionality.

Key words: Informational self-determination; consent; privacy; digital ecosystems; children and adolescents.

Kindheit unter Überwachung? Über den Schutz des Rechts auf informationelle Selbstbestimmung von Minderjährigen in digitalen Kontexten

ZUSAMMENFASSUNG

Vor dem Hintergrund der zunehmenden Digitalisierung und Konsolidierung algorithmischer Machtstrukturen analysiert diese Arbeit aus rechtsphilosophischer und menschenrechtlicher Perspektive die Neudefinition der Einwilligung von Kindern in digitalen Umgebungen als verstärkte Rechtskategorie. Ausgehend von der Untersuchung des internationalen *Corpus iuris* und regionaler Modellnormen wie der europäischen Datenschutz-Grundverordnung (DSGVO) wird argumentiert, dass die Einwilligung von Kindern und Jugendlichen nicht als reine Verfahrensformalität, sondern als substanzielle Garantie verstanden werden sollte. Der Artikel stellt ein normatives Defizit in verschiedenen lateinamerikanischen Ländern fest, insbesonde-

re in Bolivien, wo die Einwilligung von Kindern durch intransparente staatliche und unternehmerische Praktiken geschwächt wird. Demgegenüber wird eine normative Neugestaltung vorgeschlagen, die Mechanismen der wirksamen Beteiligung, der algorithmischen Verantwortung und der Bewertung der Auswirkungen auf die Menschenrechte einbezieht, die auf den Grundsätzen des Ausschusses für die Rechte des Kindes basieren, wie z. B. Datenminimierung, Transparenz und Verhältnismäßigkeit.

Schlüsselwörter: Informationelle Selbstbestimmung; Einverständnis; Privatsphäre; digitale Ökosysteme; Kinder und Jugendliche.

Introducción

En el umbral del presente siglo, la revolución digital ha permeado toda actividad humana en una suerte de *continuum* tecnológico irrefrenable, cuyo advenimiento ha incorporado una serie de *commodities* informacionales a unas interacciones sociales cada vez más automatizadas. Si bien es cierto que estos avances han facilitado, *inter alia*, el acceso a la alfabetización educativa, la participación política y la libertad de expresión de diversos grupos poblacionales –en particular, de niños, niñas y adolescentes (NNA) a través de la denominada “inclusión digital”¹ no es menos evidente que la utilización desregularizada de la cibertecnología ha traído aparejadas, a su vez, notables amenazas sobre su bienestar físico y mental, así como la exposición indebida a una serie de riesgos que se originan en el interior de los ecosistemas, como el ciberacoso, el *sexting*,² la *sextorsión*,³ el *grooming*,⁴ la pornografía extrema, la promoción del suicidio, entre otras formas de maltrato.

¹ Comité de los Derechos del Niño (CDN), Observación General No. 25 de 2 de marzo de 2021, Los derechos de los niños en relación a los entornos digitales, CRC/C/GC/25, párrafo 4, https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhqIkirKQZLK2M58RF%2F5FovEG%2BcAAx34gC78FwvnmZXGFO6kxoVqQk6dNAzT_PSRNxomyCaUSrDC%2Fod3UDPTV4yo5%2B9GMEoqMZvh9UPKTXcO12

² “El sexteo es el intercambio de imágenes o videos con contenido sexual (desnudos o casi desnudos sexualmente sugerentes) a través de teléfonos y/o Internet (mensajes, correos electrónicos, redes sociales). También puede considerarse una forma de acoso sexual en la que una niña, niño y adolescente puede ser presionado a enviar una foto a su novio/a o compañero, quien después la distribuye sin su consentimiento”. Organización de los Estados Americanos (OEA), Instituto Interamericano del Niño, la Niña y los Adolescentes, Informe regional: “Lineamientos para el empoderamiento y la protección de los derechos de los niños, niñas y adolescentes en Internet en Centroamérica y República Dominicana”, OEA/Ser.D/XXVI.18, enero de 2018, 67, <https://www.oas.org/es/sadye/publicaciones/InfRegional-ESPoo8-WEB.pdf>

³ “La sextorsión es el chantaje a niños, niñas, adolescentes, amenazándolos con difundir imágenes o videos sexuales autogenerados por estos, con la intención del extorsionador de mantener relaciones sexuales y/o continuar con la explotación sexual”. Instituto Interamericano del Niño, la Niña y los Adolescentes, Informe regional, cit., 66.

⁴ “Estrategias que realiza un adulto para ganarse la confianza de un niño, niña y adolescente, a través de Internet, con el propósito de abusarlo o explotarlo sexualmente. Es importante

En ese sentido, este trabajo tiene por objetivo analizar, en primer lugar, la fundamentación y el alcance del concepto de autonomía (como resultado de la intersección de dos vectores: racionalidad e independencia) incardinado en el ejercicio del derecho a la privacidad que les asiste a las personas menores de edad en materia de protección de datos personales que, a menudo, los entornos de realidad virtual y las aplicaciones digitales mercantilizan bajo el influjo del denominado *capitalismo cognitivo*.⁵ Seguidamente, esta investigación se enfocará en la centralidad que comporta la garantía del derecho a la privacidad de las personas menores de edad en materia de protección de datos personales, no solo para la “autonomía, la dignidad y la seguridad de los niños y el ejercicio de sus derechos”,⁶ sino también, y más importante aún, en el diseño, gestión y utilización de los dispositivos automatizados desarrollados por las *Big Tech*, que ejercen una soberanía *de facto* sobre la marea de información disponible en las plataformas digitales.⁷

Para cumplir con este propósito, propondré una serie de lineamientos rectores que los sistemas jurídicos estatales deben adoptar en la mitigación del impacto que estas actividades intrusivas generan sobre los derechos de la infancia, particularmente aquellas relacionadas con 1) la importancia del consentimiento informado para procesar los datos de NNA al amparo de los estándares internacionales desarrollados en este campo; 2) las transformaciones que la concepción de privacidad atraviesa al interior de los ecosistemas digitales estructurados por arquitecturas algorítmicas de control;⁸ y 3) la falta de sujeción normativa del sector privado en materia de tratamiento de datos personales de la infancia conforme a los principios rectores desarrollados por el Comité de los Derechos del Niño (Comité DN), tales como minimización de datos, transparencia, proporcionalidad y debida diligencia empresarial.⁹ Finalmente, incidiré, a manera de colofón, sobre la dimensión ética que debe incorporar el desarrollo de las nuevas tecnologías, principalmente en lo que concierne a la recolección de datos masivos o residuales de las poblaciones infantiles.

expresar que siempre es un adulto quien ejerce el *grooming*”. Instituto Interamericano del Niño, la Niña y los Adolescentes, Informe regional, cit., 66.

⁵ José María Lassalle, *Ciberleviatán. El colapso de la democracia liberal frente a la revolución digital* (Barcelona: Arpa Editores, 2019), 22.

⁶ CDN, Observación General No. 25, cit., párrafo 67.

⁷ Lassalle, *Ciberleviatán...*, 91.

⁸ Lassalle sostiene que la sociedad contemporánea se encuentra inmersa en una *civilización artificial* donde “la racionalidad tecnodigital ha capturado los fundamentos de la autonomía” y “el algoritmo ha sustituido al juicio moral”. José María Lassalle, *Civilización artificial* (Barcelona: Arpa Editores, 2024), cap. 3.

⁹ Toda arquitectura normativa que pretenda limitar la injerencia del sector privado en la esfera informacional infantil debe fundarse en una concepción robusta del interés superior, la lógica restrictiva de minimización de datos y un principio de diligencia ética y jurídica frente a las nuevas formas de vulnerabilidad digital.

1. Metodología

En esta investigación se emplea una metodología cualitativa de carácter analítico-interpretativo, orientada al examen de los distintos –aunque interrelacionados– marcos normativos, doctrinarios y jurisprudenciales que regulan el derecho a la privacidad y la protección de datos personales de NNA en contextos digitales. Este enfoque se sustenta en el uso de técnicas hermenéuticas propias del análisis jurídico, las cuales permiten desentrañar el contenido sustantivo de las normas internacionales de derechos humanos, en especial aquellas emanadas de los sistemas universal y regional de protección, así como su articulación con los desafíos tecnológicos contemporáneos derivados de la denominada “economía de datos”.

2. Autonomía, soberanía informacional infantil y relectura constitucional de la privacidad en la era algorítmica

En la era del *big data*, la ubicuidad de las plataformas tecnológicas en las interacciones humanas ha transformado radicalmente los modos de recolección, almacenamiento y explotación de datos personales, particularmente entre poblaciones vulnerables, como NNA. Los códigos normativos de esta nueva cultura digital, vertebrada por arquitecturas algorítmicas, han cristalizado una suerte de *metademocracia virtual*,¹⁰ caracterizada, entre otros elementos, por la disputa hegemónica del significado de la verdad en contextos de comunicación hipermediada. Es precisamente en este terreno semiótico de *posverdad* donde “toda racionalidad de la acción comunicativa pierde significado”¹¹ frente a la infoxicación de lo real, extinguiéndose de esa manera cualquier atisbo de deliberación crítica.¹²

En este escenario, el derecho a la privacidad no puede ser concebido como un reducto estrictamente individualista, sino como un “poder fundamental”¹³ estructurante de la autonomía relacional, entendida no solo como libertad negativa frente a interferencias externas, sino como la capacidad moral y política para controlar activamente el flujo de información personal sin interferencias arbitrarias (i. e.,

¹⁰ María del Pilar García Pachón, ed., *Información, participación y justicia ambiental: herramientas para alcanzar el desarrollo sostenible en la democracia ambiental* (Bogotá: Universidad Externado de Colombia, 2020), 171.

¹¹ García Pachón, *Información, participación...*, 171.

¹² José Ignacio Niño González, Mario Barquero Cabrero y Enrique García García, “Opinión pública e infoxicación en las redes: los fundamentos de la post-verdad”, *Vivat Academia* 139 (2017): 83-94, <https://www.redalyc.org/journal/5257/525754431007/html/>

¹³ Carissa Véliz, *Privacidad es poder: datos, vigilancia y libertad en la era digital* (Santiago de Chile: Ediciones Debate, 2021), 14.

libertad republicana).¹⁴ Retomemos la formulación clásica de Nissenbaum sobre privacidad como “integridad contextual”:

Además de la relación causal o habilitante entre la privacidad y la autonomía, existe una conexión adicional, de carácter constitutivo, que rara vez es reconocida como tal y que desempeña un papel esencial en la definición más ampliamente aceptada del derecho a la privacidad: *el derecho a controlar la información relativa a uno mismo*. La plausibilidad de este derecho a controlar la información personal –incluso cuando se encuentra limitado y condicionado por otros derechos y obligaciones que compiten o contrapesan– descansa en la premisa de que la información sobre nosotros constituye un ámbito respecto del cual los individuos pueden ejercer autonomía. En este sentido, es comparable con los derechos *prima facie* de autodeterminación que poseemos sobre nuestros cuerpos y sobre el acceso a los mismos.¹⁵

Pero esta concepción se ha visto erosionada ante el “giro inferencial” (*inferential turn*) en el tratamiento de datos, donde el riesgo ya no reside exclusivamente en la divulgación voluntaria de información, sino en las capacidades predictivas que terceros –especialmente actores privados, como Meta, Google, Tik Tok, X– pueden ejercer a partir de trazas digitales aparentemente neutras.¹⁶

En el nuevo ecosistema digital, la construcción del consentimiento ha dejado de ser un acto volitivo aislado para convertirse en una decisión condicionada por estructuras algorítmicas de asimetría informativa, diseñadas para maximizar la

¹⁴ El concepto de ‘libertad republicana’ entendida como “ausencia de dominación” ha sido defendido, a decir de Spector, por autores como Philip Pettit y Quentin Skinner, quienes abogan por una “independencia estructural” del individuo en el interior de una comunidad política dotada de instituciones “capaces de anular la capacidad de las personas de interferirse arbitrariamente entre sí”. Ezequiel Spector, *La libertad entendida como cooperación social. Una teoría de la democracia liberal* (Barcelona: Marcial Pons, 2025), 27, 57-58.

¹⁵ Helen Nissenbaum, “Privacy as Contextual Integrity”, *Washington Law Review* 79 (2004): 149, <https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10>. A este respecto, en el asunto *Centre for Child Law and Others v Media 24 Limited and Others*, la Corte Constitucional sudafricana determinó: “Siempre que una persona tenga la facultad de decidir qué desea divulgar al público y resulte razonable la expectativa de que dicha decisión será respetada, entra en juego el derecho a la privacidad” (traducción propia). *Centre for Child Law and Others v Media 24 Limited and Others* (CCT261/18) [2019] ZACC 46; 2020 (3) BCLR 245 (CC); 2020 (1) SACR 469 (CC); 2020 (4) SA 319 (CC) (4 de diciembre de 2019), <https://www.saflii.org/za/cases/ZACC/2019/46.html>.

¹⁶ Nissenbaum, “Privacy as Contextual Integrity”, 105. A este respecto, en su famosa obra, la socióloga estadounidense Shoshana Zuboff describe de qué manera las “behavioral surplus data” (excedente conductual) surgen de las trazas digitales como materia prima para el capitalismo de datos, esto es, bajo una lógica acumulativa dentro de un “behavioral futures markets” (mercado de futuros conductuales). Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: PublicAffairs, 2019), edición en PDF, cap 3.

extracción desautorizada de datos antes que para preservar la agencia del sujeto. La privacidad infantil,¹⁷ en ese contexto, se ve crecientemente amenazada por el fenómeno de la “economía del perfilado” (*profiling economy*),¹⁸ donde la segmentación conductual reemplaza al reconocimiento jurídico, y los datos personales se convierten en insumos estratégicos (“materia prima”) para un modelo de negocios basado esencialmente en la “violación masiva de derechos”.¹⁹

Esta realidad no solo desborda las categorías normativas tradicionales de “consentimiento” y “vida privada”, sino que exige una relectura constitucional donde el derecho a la privacidad se asuma como autodeterminación informacional, esto es, como el derecho de toda persona, indistintamente de su rango etario,²⁰ a tener control efectivo y comprensible sobre la circulación, tratamiento y uso de sus datos personales. Por ello, el desafío contemporáneo al que asistimos no radica únicamente en la revelación voluntaria de información, sino en los conocimientos que terceros –particularmente corporaciones– pueden inferir a partir de datos residuales aparentemente no sensibles (v. gr., metadatos de navegación, registros de ubicación, patrones de actividad en redes sociales, uso de aplicaciones bancarias, huellas de consumo digital, etc.), erosionando así la frontera entre lo público, lo íntimo y lo calculable.²¹ El consentimiento, en ese marco, deja de ser garantía y se convierte en un frágil ritual –cuasificcional– frente al diseño opaco que comportan las plataformas digitales.²²

Desde esta perspectiva, la niñez no puede ser tratada como un objeto pasivo de protección normativa *tout court*, sino como un sujeto (activo) de derechos informacionales, cuya incipiente autonomía exige salvaguardias reforzadas frente a estructuras tecnológicas que operan como dispositivos de poder sin control democrático. Este ámbito hiperconectado no solo cosifica al ser humano, sino que también reproduce y perpetúa una suerte de “paternalismo tecnológico” que socava la

¹⁷ “La privacidad es vital para la autonomía, la dignidad y la seguridad de los niños y para el ejercicio de sus derechos”. Comité de los Derechos del Niño de las Naciones Unidas, Observación General No. 25, cit., párrafo 69. En el mismo sentido, United Nations General Assembly (UNGA), Resolution on the Right to Privacy in the Digital Age, A/RES/73/179, December 17, 2018, https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/73/179

¹⁸ Eduard Fosch-Villaronga et al., *The Chilling Effects of Algorithmic Profiling and Automated Decision-Making*, eLaw Working Paper Series (Leiden: Universiteit Leiden, 2020), 19, <https://www.universiteitleiden.nl/binaries/content/assets/rechtsgeleerdheid/instituut-voor-metajuridica/elaw-working-paper-series/wps2020.001.fosch-the-chilling-effects-of-algorithmic.pdf>

¹⁹ Véliz, *Privacidad...*, 188.

²⁰ Ello no implica, como se demostrará *infra*, que aquellos grupos en situación de especial vulnerabilidad (v. gr., población infantil), no sean objeto de “medidas reforzadas” o de “atención prioritaria” por parte de las políticas estatales.

²¹ Jens-Erik Mai, “Situating Personal Information: Privacy in the Algorithmic Age”, en *Human Rights in the Age of Platforms*, ed. por Rikke Frank Jørgensen (Cambridge, MA: MIT Press, 2019), 105.

²² Mai, “Situating Personal Information: Privacy in the Algorithmic Age”, 101.

autonomía individual y priva a las personas del derecho fundamental a la intimidad, esto es, de la “parte sensible que lo constituye”.²³

Autores como Byung-Chul Han han advertido, en línea con lo anterior, que esta transformación digital implica una “mutación identitaria” en el sujeto contemporáneo, cuya esfera individual se ve desarticulada bajo el influjo de un nuevo contrato social administrado por algoritmos, que predice y moldea conductas mediante lenguajes artificiales que no requieren violencia o legitimación para ser efectivos, tan solo estímulo.²⁴ Esta suplantación tecnopolítica de la agencia –mediada por arquitecturas persuasivas invisibles (v. gr., sistemas de recomendación en redes sociales, motores de búsqueda “personalizados”, publicidad dirigida, etc.)– introduce riesgos sistémicos sobre la capacidad resolutoria del agente moral,²⁵ especialmente cuando se trata de sujetos en desarrollo, como NNA.

En este marco, las consecuencias sobre la infancia no solo replican los efectos disruptivos que estas dinámicas generan sobre los adultos, sino que los amplifican. Como se dijo anteriormente, si bien los entornos digitales han incrementado el acceso a bienes sociales fundamentales como la educación o la conectividad,²⁶ también han intensificado el rastreo y la explotación de la huella digital de NNA mediante el uso de técnicas corrosivas de seguimiento (*data tracking*), impactando de forma silenciosa su bienestar psicosocial.

²³ Lassalle, *Ciberleviatán...*, 21.

²⁴ Lassalle, *Ciberleviatán...*, 19-20.

²⁵ “Esta condición netamente kantiana en su formulación originaria, ha sido enriquecida por ulteriores desarrollos relativos a las posibilidades de la acción racional, en la medida en que va precedida de un proceso de *singularización de los deseos o preferencias, seguido de otro proceso de jerarquización de las mismas*. Esta compleja tarea que cada sujeto realiza comprometiendo su capacidad de reflexión comporta evaluar, calibrar, sopesar y finalmente asignar un orden de prioridades; orden que, a su vez, responderá a pautas que revelan la disposición moral y emocional del sujeto”. Silvina Álvarez Medina, “Derechos humanos emergentes: fundamentación, contenido y sujetos desde una perspectiva de género”, en *Repensar los derechos humanos*, ed. por Ángeles Ródenas (Lima: Palestra Editores, 2018), 336-337. Énfasis agregado. Por su parte, Carissa Véliz sostiene: “En las democracias liberales, con muy pocas excepciones, nadie –ni siquiera el Estado– puede decirte qué pensar, qué decir, qué hacer para ganarte la vida, con quien relacionarte, ni cómo pasar el tiempo. Tú decides todas esas cosas y más. Sin autonomía, no tienes libertad, porque tu vida está controlada por otros. *Tener autonomía significa tener poder sobre tu propia vida*”. Véliz, *Privacidad...*, 87.

²⁶ Por ejemplo, el Plan de conectividad educativa de informática básica para el aprendizaje en línea (Plan Ceibal), implementado en el Uruguay a partir del año 2007, ha posibilitado –en términos de equidad– el desarrollo de *capacidades digitales* en favor de niños, niñas y adolescentes que, de otra manera, no podrían acceder a estos recursos debido a su “inserción social desfavorable”. Ana Rivoir y Susana Lamschtein, “Plan Ceibal, un caso de usos de las tecnologías de información y de las comunicaciones en la educación para la inclusión social”, en *Las tecnologías digitales frente a los desafíos de una educación inclusiva en América Latina: algunos casos de buenas prácticas*, ed. por Guillermo Sunkel y Daniela Trucco (Santiago de Chile: Comisión Económica para América Latina y el Caribe, 2012), 170, <https://repositorio.cepal.org/server/api/core/bitstreams/7be78858-1bdf-4c59-b7d2-78532198900b/content>

Estos procesos –cuyos riesgos fueron detectados, *inter alia*, por las relatorías especiales de la Organización de las Naciones Unidas (ONU)–²⁷ se manifiestan en la inhibición del desarrollo de competencias digitales apropiadas para su edad y madurez, así como en la exposición a discursos discriminatorios (como aquellos propagados en la *manosfera*²⁸), que configuran nuevas formas de violencia simbólica y estructural, donde el mayor número de víctimas son niñas y mujeres adolescentes.²⁹ A este respecto, el Informe temático de la Plataforma de Mecanismos de Expertos Independientes sobre la Discriminación y la Violencia contra la Mujer (EDVAW) de 2022 ha establecido:

La dimensión digital de la violencia contra la mujer es alarmantemente frecuente. Según un estudio de 2015 realizado por la Comisión de Banda Ancha para el Desarrollo Sostenible de las Naciones Unidas, casi tres cuartas partes de las mujeres han experimentado algún tipo de violencia de género en línea, y casi dos tercios de los autores son hombres [...]. En 2020, un estudio de la *Economist Intelligence Unit* que abarcó 45 países reveló que el 85% de las mujeres ha experimentado o presenciado violencia en línea y facilitada por

²⁷ “La injerencia indebida en la intimidad de las personas puede limitar en forma tanto directa como indirecta el libre intercambio y evolución de ideas. Las restricciones al anonimato de las comunicaciones, por ejemplo, tienen un efecto intimidatorio en las víctimas de todas las formas de violencia y abuso, que podrían ser renuentes a denunciarlas por temor a la doble victimización”. Naciones Unidas, Consejo de Derechos Humanos, Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, Frank La Rue, A/HRC/23/40, 17 de abril de 2013, párrafo 24.

²⁸ Un neologismo con el que se hace referencia “al conjunto de comunidades de hombres en Internet organizados en distintas subculturas como MRA (*Men Rights Activists*); MT-GOW (*Men Going Their Own Way*); o Incels (*Involuntary Celibats*)”. Para una comprensión más minuciosa en torno a esta “tribu digital” y sus repercusiones en términos sociológicos y jurídicos, ver European Commission, *Incels: A First Scan of the Phenomenon (in the EU) and its Relevance and Challenges for P/CVE* (Luxembourg: Publications Office of the European Union, 2021), https://home-affairs.ec.europa.eu/system/files/2021-10/ran_incels_first_scan_of_phenomen_and_relevance_challenges_for_p-cve_202110_en.pdf. En el campo narrativo-audiovisual, una sugestiva radiografía sobre la temprana configuración del espectro identitario y los impactos negativos que el uso desregulado de las redes de interacción virtual trae consigo sobre el bienestar psicosocial de NNA, puede encontrarse en la serie *Adolescence*, distribuida por la plataforma Netflix.

²⁹ “Más allá del problema del acceso, la falta de alfabetización digital agrava las cuestiones relacionadas con la privacidad de los menores de edad. Dicha carencia dificulta su capacidad para desenvolverse eficazmente en las redes sociales, desarrollar y crear contenidos, acceder a información de valor, distinguir y denunciar contenidos perjudiciales ante las plataformas de redes sociales y los intermediarios de Internet, entre otras problemáticas” (traducción propia). Yohannes Eneyew, Valerie Verdoodt y Eva Lievens, “General Comment No. 25 on Children’s Rights in Relation to the Digital Environment: Implications for Children’s Right to Privacy and Data Protection in Africa”, *Human Rights Law Review* 24, n.º 3 (2024): 65, <https://doi.org/10.1093/hrlr/ngae018>

la tecnología, desde el 74% en Europa, el 91 % en América Latina y el Caribe y el 90% en África.³⁰

Frente a esta acuciante realidad, las respuestas institucionales han surgido desde el sistema universal de protección de derechos humanos, particularmente de sus órganos de tratado. Así, el Comité DN ha emitido pronunciamientos clave que establecen deberes concretos para los Estados y para los actores privados con relación a la protección de los derechos de los niños. Por ejemplo, la Observación General No. 25 (2021) sobre los derechos de los niños en relación con los entornos digitales (OG-25) explicita –en línea con el artículo 16 de la Convención de Naciones Unidas sobre los Derechos del Niño de 1989 (CDN)– que “la privacidad es vital para la autonomía, la dignidad y la seguridad de los niños y para el ejercicio de sus derechos”,³¹ precisando además que “toda injerencia debe sujetarse a criterios de legalidad, proporcionalidad y finalidad legítima”.³²

Por su parte, la Observación General No. 16 (2013) sobre las obligaciones del Estado en relación con el impacto del sector empresarial en los derechos del niño

³⁰ Consejo de Europa, “La dimensión digital de la violencia contra la mujer abordada por los siete mecanismos de la Plataforma EDVAW” (documento temático de la Plataforma de Mecanismos de Expertos Independientes sobre la Discriminación y la Violencia contra la Mujer, EDVAW, noviembre de 2022), 9, <https://rm.coe.int/la-dimension-digital-de-la-violencia-contra-la-mujer-abordada-por-los-/1680a933ad>. “Otras fuentes señalan que 23% de las mujeres han experimentado acoso en línea al menos una vez en su vida, y se estima que una de cada diez mujeres ya había sufrido alguna forma de ciberviolencia desde los 15 años de edad”. Organización de los Estados Americanos (OEA), *La violencia de género en línea contra las mujeres y niñas: Guía de conceptos básicos, herramientas de seguridad digital y estrategias de respuesta*, OEA/Ser.D/XXV.25, <https://www.oas.org/es/cim/docs/ViolenciaGeneroLineaGUIA-ES.pdf>

³¹ Al respecto, en el Caso Artavia Murillo y otros vs. Costa Rica, la Corte Interamericana de Derechos Humanos sostuvo que “la vida privada engloba aspectos de la identidad física y social, incluyendo el derecho a la autonomía personal, desarrollo personal y el derecho a establecer y desarrollar relaciones con otros seres humanos y con el mundo exterior”. Corte IDH, Artavia Murillo y otros (“Fecundación *in vitro*”) vs. Costa Rica, Sentencia de 28 de noviembre de 2012, Excepciones Preliminares, Fondo, Reparaciones y Costas, Serie C, No. 257, párrafo 143, https://www.corteidh.or.cr/docs/casos/articulos/seriec_257_esp.pdf. Por otro lado, en el Caso Fontevecchia y D’Amico vs. Argentina, este tribunal resolvió que “el Estado tiene la obligación de garantizar el derecho a la vida privada mediante acciones positivas, lo cual puede implicar, en ciertos casos, la adopción de medidas dirigidas a asegurar dicho derecho protegiéndolo de las interferencias de las autoridades públicas, así como también de las personas o instituciones privadas, incluyendo los medios de comunicación”. Corte IDH, Caso Fontevecchia y D’Amico vs. Argentina, Sentencia de 29 de noviembre de 2011, Fondo, Reparaciones y Costas, Serie C, No. 238, párrafo 49, https://corteidh.or.cr/docs/casos/articulos/seriec_238_esp.pdf

³² En palabras del Comité, “la injerencia en la vida privada de un niño solo es admisible si no es arbitraria o ilegal. Por tanto, toda injerencia de este tipo debe estar prevista por la ley, tener una finalidad legítima, respetar el principio de *minimización de los datos*, *ser proporcionada*, *estar concebida en función del interés superior del niño* y no debe entrar en conflicto con las disposiciones, los fines o los objetivos de la Convención”. CDN, Observación General No. 25, cit., párrafo 69.

(OG-16) consagra un estándar reforzado de “diligencia debida” que los Estados deben imponer al sector empresarial, a fin de que este “identifique, prevenga y mitigue el impacto de sus operaciones”, especialmente aquellas que comporten carácter comercial.³³ Esta exigencia no puede diluirse dentro de los esquemas generales de derechos humanos, sino que debe preservar la especificidad normativa de la CDN y sus protocolos complementarios,³⁴ garantizando así una “consideración especial hacia los efectos diferenciados sobre los niños”.³⁵

Adicionalmente, la Observación General No. 7 del Comité Africano de Expertos sobre los Derechos y Bienestar del Niño (ACERW por sus siglas en inglés) ha propuesto un “enfoque sensible” (*sensitive approach*), capaz de armonizar “el derecho a la privacidad del menor y su capacidad evolutiva” con la “responsabilidad parental y el deber de guiar a los hijos en su comportamiento”, bajo el criterio del interés superior del menor (*best interests*).³⁶ De acuerdo con este pronunciamiento, “los padres deberían estar capacitados para orientar y asesorar a sus hijos en materia de seguridad en línea, en lugar de bloquear por completo su acceso al entorno digital, dado que los dominios en línea y fuera de línea están cada vez más entrelazados y no pueden separarse con facilidad”.³⁷ Una ilustración concreta de este balance puede identificarse en la OG-25 antes apuntada cuando establece lo siguiente:

Los Estados partes deben tener en cuenta que el apoyo y la orientación que se presten a los padres y cuidadores deben basarse en la comprensión de la especificidad y singularidad de las relaciones entre padres e hijos. Esa orientación debe ayudar a los padres a mantener un equilibrio adecuado entre la protección del niño y su incipiente autonomía, basándose en la empatía y el respeto mutuos más que en la prohibición o el control. *Para ayudar a los padres y cuidadores a mantener un equilibrio entre las responsabilidades parentales y*

³³ CDN, Observación General No. 16 de 17 de abril de 2013, Sobre las obligaciones del Estado en relación con el impacto del sector empresarial en los derechos del niño, CRC/C/GC/16, párrafo 62, <https://www.plataformadeinfancia.org/wp-content/uploads/2018/09/observacion-general-16-obligaciones-estado-relacion-con-impacto-sector-empresarial-derechos-nino-2013-.pdf>

³⁴ A saber: Protocolo Facultativo relativo a la participación de niños en conflictos armados (2000); Protocolo Facultativo sobre la venta de niños, la prostitución infantil y la utilización de niños en la pornografía (2000); y Protocolo Facultativo relativo a un procedimiento de comunicaciones (2011).

³⁵ CDN, Observación General No. 16, cit., párrafo 63.

³⁶ African Committee of Experts on the Rights and Welfare of the Child (ACERWC), General Comment No. 7 on Article 27 of the ACRWC: “Sexual Exploitation” de 21 de julio de 2022, párrafo 61, https://reporting.acerwc.africa/sites/default/files/2022-09/General-Comment-on-Article-27-of-the-ACRWC_English_o.pdf. En el mismo sentido, Eneyew *et al.*, “General Comment No. 25 on Children’s Rights in Relation to the Digital Environment: Implications for Children’s Right to Privacy and Data Protection in Africa”, 12-13.

³⁷ ACERWC, General Comment No. 7, cit., 12-13. Traducción propia. Énfasis agregado.

*los derechos del niño, los principios rectores deben ser el interés superior del niño, junto con la consideración de la evolución de sus facultades.*³⁸

Así, a partir de estas nuevas directivas interpretativas de vocación regional y universal, la protección de la privacidad infantil –que integra, entre otros elementos, el respeto por la dignidad, la integridad personal y la autonomía individual–³⁹ debe entenderse como la piedra de toque para la formación de agentes libres, capaces de autodeterminar su biografía digital. Su exigibilidad no se agota, por tanto, en los dispositivos de control parental, sino que requiere una arquitectura institucional robusta que reconozca a los NNA la soberanía informacional como un elemento indispensable de su desarrollo, máxime en un escenario donde, como ocurre actualmente, el consentimiento es extremadamente difuso y el poder algorítmico es estructural.

3. Sobre la importancia del consentimiento: autodeterminación informativa y garantías institucionales para una infancia digital

En los actuales entornos de realidad virtual, el consentimiento ha dejado de ser una mera formalidad legal para devenir en una expresión compleja de autodeterminación personal, especialmente en el caso de NNA. En lugar de considerarse como un acto voluntario aislado, el consentimiento debe ser concebido como una construcción progresiva de autonomía en contextos mediados por infraestructuras tecnológicas opacas, diseñadas –como fue señalado *ut supra*– para la recopilación de datos y la extracción de valor informacional con fines lucrativos mediante procesos de predictibilidad algorítmica.

Esta evolución conceptual se encuentra anclada, además de los fundamentos teóricos arriba expuestos, en los marcos regulatorios fundacionales de la protección de datos, particularmente en las *Fair Information Practices* (FIPs) desarrolladas en la década de los setenta,⁴⁰ cuando el consentimiento fue articulado inicialmente como

³⁸ CDN, Observación General No. 25, cit., párrafo 86. Énfasis agregado.

³⁹ Constitutional Court of South Africa, *Centre for Child Law and Others v Media 24 Limited and Others*, Sentencia de 4 de diciembre de 2019, ZACC 46, párrafo 49, <https://www.saflii.org/za/cases/ZACC/2019/46.html>

⁴⁰ “Cada vez que una persona descarga una nueva aplicación en su teléfono, se le solicita que acepte sus términos del servicio. Ello obedece a una preocupación que se remonta a los primeros tiempos, cuando la comunidad internacional advirtió los riesgos derivados de la digitalización de los datos personales y elaboró, en 1973, los Principios de Información Justa (Fair Information Principles o Fair Information Practice Principles, comúnmente conocidos como FIPs) con el fin de hacerles frente. Con el paso del tiempo, los FIPs se han ido convirtiendo en sinónimo del derecho a la privacidad. Tal como su denominación lo indica, los FIPs tienen como objetivo garantizar la equidad en las prácticas relacionadas con la información

la “base legitimadora primaria” (*primary legitimizing basis*)⁴¹ del tratamiento de datos personales, dotándolo de una función estructural dentro del emergente ecosistema normativo.⁴² Este trasfondo exige, por tanto, una reconceptualización multinivel y descompartimentalizada⁴³ del consentimiento (esto es, donde los estándares universales y regionales puedan converger asociativamente) como derecho sustantivo y no meramente procedimental, cuyo ejercicio se halla actualmente amenazado por las lógicas totalizantes de los entornos de simulación y mediación digital.

Desde esta perspectiva, y en consonancia con el *principio de autonomía progresiva* consagrado en el artículo 5 de la CDN, el consentimiento infantil no puede interpretarse como un simple acto contractual;⁴⁴ requiere, asimismo, condiciones materiales e institucionales que garanticen su ejercicio libre, informado y evolutivamente adecuado. En esa línea, la OG-25 ha establecido que dicho consentimiento debe tener en cuenta el grado de madurez del niño, la inteligibilidad del entorno y la capacidad

personal de las personas” (traducción propia). Ignacio Cofone, *The Privacy Fallacy: Harm and Power in the Information Economy* (Cambridge: Cambridge University Press, 2024), edición en PDF, 13.

⁴¹ “La mayoría de las jurisdicciones a nivel mundial han incorporado los FIPs, y en particular su principio de tratamiento lícito, leal y transparente de los datos personales, mediante una disposición clave en sus legislaciones de protección de datos que exige el consentimiento individual para el tratamiento de dichos datos. Así, por ejemplo, el consentimiento constituye la principal base legitimadora para el tratamiento de datos en Andorra, Argentina, Brasil, Canadá, las Islas Feroe, Guernsey, Japón, Corea, México, Singapur y Uruguay. El consentimiento es un elemento central del derecho de protección de datos en todo el mundo, especialmente fuera de Europa” (traducción propia). Cofone, *The Privacy Fallacy*..., 89.

⁴² Durante los últimos años, el paradigma sobre el que se asientan las FIPs ha sido calificado, sin perjuicio de lo expuesto supra, como “tradicionalista” e “insuficiente”. A decir de Cofone, “Diseñados en una época anterior a que las personas dispusieran de ordenadores en sus hogares, y mucho menos de acceso a Internet, los FIPs tenían como finalidad proteger a las personas en un entorno radicalmente distinto del actual ecosistema informativo impulsado por la inteligencia artificial. Desde entonces, estos principios han sido objeto de severas críticas por parte de la doctrina especializada en materia de privacidad” (traducción propia). Por ello, el autor señala que la solución adecuada a este asunto “no es únicamente modificar los FIPs, sino de transformar los fundamentos estructurales que les sirven de soporte” (traducción propia). Cofone, *The Privacy Fallacy*..., 15.

⁴³ Laurence Burgorgue-Larsen, “Decomartmentalization: The key technique for interpreting regional human rights treaties”, *International Journal of Constitutional Law* 16, n.º 1 (2018): 187-213, <https://doi.org/10.1093/icon/moy010>

⁴⁴ Organizaciones como 5Rights Foundation han señalado que los sistemas de verificación de consentimiento implementados por numerosas plataformas tecnológicas (v. gr., Google, Meta o TikTok) operan bajo un diseño legal estandarizado que simula una manifestación de voluntad, pero que en realidad no garantiza el control ni la comprensión efectiva de los menores sobre el uso de sus datos personales. 5Rights Foundation, “A High Level of Privacy, Safety and Security for Minors: A Best Practices Baseline for the Implementation of the Digital Services Act for Children”, febrero de 2024, 12.

efectiva para comprender las implicancias que conlleva el tratamiento de datos.⁴⁵ De ahí que la protección infantil no puede limitarse a meras advertencias o a formularios de aceptación pasiva al momento de acceder, por caso, a los contenidos provistos por las aplicaciones digitales (i. e., Facebook, Instagram, WhatsApp, Telegram), sino que debe operar a través de estructuras comunicacionales asequibles y mecanismos de reversibilidad que devuelvan al menor el control sobre su identidad digital.⁴⁶

A ello debe sumarse una aproximación normativa mucho más robusta. Siguiendo la teoría de la justicia como equidad de John Rawls, la autonomía –y, por extensión, el consentimiento– no puede constituir una ilusión sostenida por asimetrías informativas o coacciones estructurales. Por el contrario, debe reflejar condiciones de imparcialidad e igualdad deliberativa (esto es, tanto a nivel decisional como interactiva), donde el sujeto pueda aceptar libremente los principios que rigen su participación en el entorno social y, en este caso, digital.⁴⁷ Para ser válido constitucionalmente, el consentimiento infantil debe operar, entonces, dentro de un marco institucional que lo proteja de la lógica tecnocrática del mercado en arreglo a los principios de minimización de datos,⁴⁸ interés superior, transparencia, proporcionalidad, participación y autonomía progresiva.

Este conjunto de criterios guarda relación con los Principios Actualizados sobre la Privacidad y la Protección de Datos Personales adoptados por el Comité Jurídico Interamericano (CJI) de la Organización de los Estados Americanos (OEA), cuyo sustrato explicita:

... los recopiladores y Encargados de Datos [deberán ...] hacer un esfuerzo razonable para cerciorarse de que los Datos Personales que manejen correspondan al mínimo requerido para la finalidad expresa. En algunos sistemas

⁴⁵ En términos del propio Comité, “cuando se solicite el consentimiento para procesar los datos de un niño, los Estados partes deben cerciorarse de que el niño o, según su edad y el grado de evolución de sus facultades, el padre o el cuidador, den su consentimiento informado, libre y previo al procesamiento de esos datos”, además de proporcionar informaciones sobre estas cuestiones “en un lenguaje adaptado a los niños y en formatos accesibles”. CDN, Observación General No. 25, cit., párrafos 71 y 72; 5Rights Foundation, “A High Level of Privacy, Safety and Security for Minors: A Best Practices Baseline for the Implementation of the Digital Services Act for Children”, 12.

⁴⁶ 5Rights Foundation, “A High Level of Privacy, Safety and Security for Minors: A Best Practices Baseline for the Implementation of the Digital Services Act for Children”, 12.

⁴⁷ John Rawls, *A Theory of Justice* (Cambridge, MA: Harvard University Press, 1971), 266-273 (autonomía moral) y 118-130 (posición original y consentimiento).

⁴⁸ De acuerdo con las Recomendaciones de la Comisión Nacional de Informática y Libertades (Francia) sobre los derechos digitales de los niños (2021), el principio de minimización implica que todo sistema de verificación de edad y consentimiento parental debe estar diseñado con la finalidad de “limitar la recopilación de datos personales a lo estrictamente necesario”, de manera que no se conserven e instrumentalicen para otros fines, particularmente de carácter comercial. 5Rights Foundation, “A High Level of Privacy, Safety and Security for Minors: A Best Practices Baseline for the Implementation of the Digital Services Act for Children”, 17.

jurídicos se usa el concepto de “proporcionalidad” para hacer referencia al equilibrio de valores en pugna. La proporcionalidad requiere que las instancias decisorias determinen si una medida ha ido más allá de lo que se requiere para alcanzar una finalidad legítima y si los beneficios alegados excederán los costos previstos.⁴⁹

Por consiguiente, los Estados tienen el deber de asegurar, por un lado, “que los proveedores de servicios digitales respeten las directrices, normas y códigos pertinentes”⁵⁰ –específicamente en lo atinente a los efectos negativos que la mercadotecnia y la publicidad puedan generar sobre los derechos de la niñez–⁵¹ y de aplicar, por otro, “normas de moderación de contenidos lícitas, necesarias y proporcionadas”,⁵² procurando que “los controles de contenido, los sistemas de filtrado escolar y otras tecnologías orientadas a la seguridad, no se utilicen para restringir el acceso de los niños a la información en el entorno digital, sino únicamente para evitar que el material nocivo llegue a [ellos]”.⁵³

A este respecto, en el año 2021, el Informe del Relator Especial sobre el derecho a la privacidad, Joseph A. Cannataci reveló cómo durante la pandemia del covid-19, diversas plataformas educativas utilizaron a NNA como fuentes de datos masivos sin garantías adecuadas. En este contexto, el consentimiento infantil se mostró incapaz de resistir prácticas subrepticias como el rastreo por terceros o la comercialización de metadatos.⁵⁴ La consecuencia no solo ha sido una afectación a la privacidad infantil, sino también a las dimensiones fundamentales del desarrollo psicosocial de este grupo, incluyendo su autoestima, seguridad emocional

⁴⁹ Organización de los Estados Americanos (OEA), Comité Jurídico Interamericano (CJI), Principios actualizados sobre la privacidad y la protección de datos personales, OEA/Ser.D/XIX.20, diciembre de 2021. <https://www.oas.org/ext/DesktopModules/MVC/OASD-nnModules/Views/Item/Download.aspx?type=1&id=1185&lang=2>. Para una comprensión, *lato sensu*, de la aplicación del principio de proporcionalidad en contextos de injerencia al ejercicio del derecho a la intimidad y, por extensión, a la protección de datos personales, ver Tribunal de Justicia de la Unión Europea (TJE), *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others*, Sentencia de 8 de abril de 2014, Asunto C-293/12, párrafos 45-69, <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62012CJ0293>. En cuanto a la “supresión” y el “almacenamiento” de datos por parte de las “plataformas comunicacionales” que operan dentro del comercio electrónico, ver TJE, *Eva Glawischmig-Piesczek contra Facebook Ireland Limited*, Sentencia de 3 de octubre de 2019, Asunto C-18/18, <https://curia.europa.eu/juris/document/document.jsf?text=&docid=218621>

⁵⁰ CDN, Observación General No. 25, cit., párrafo 56.

⁵¹ CDN, Observación General No. 16, cit., párrafos 19 y 59.

⁵² CDN, Observación General No. 25, cit., párrafo 56.

⁵³ CDN, Observación General No. 25, cit., párrafo 56.

⁵⁴ Asamblea General de las Naciones Unidas, Informe del Relator Especial sobre el derecho a la privacidad, Joseph A. Cannataci. Derecho a la privacidad, A/76/220, 23 de julio de 2021, párrafo 9, <https://documents.un.org/doc/undoc/gen/n21/203/69/pdf/n2120369.pdf>

y percepción de agencia personal,⁵⁵ donde los jóvenes pertenecientes al colectivo LGBTQI se han mostrado particularmente afectados.⁵⁶

Como ha sostenido la Corte Interamericana de Derechos Humanos (Corte IDH), el consentimiento, para ser jurídicamente válido, debe reunir condiciones de libertad, información suficiente, ausencia de coacción e inteligibilidad según la situación del titular del derecho, pudiendo ser revocado en cualquier momento.⁵⁷ Esto debido a que los grupos en situación de especial vulnerabilidad (v. gr., personas menores de edad) requieren medidas de protección reforzadas⁵⁸ para ejercer, por ejemplo, un consentimiento auténtico, que no solo compensen las asimetrías estructurales, sino que también habiliten el ejercicio efectivo de sus derechos fundamentales de

⁵⁵ “Alrededor del 25 % de los adolescentes de entre 13 y 17 años han comunicado haber recibido imágenes explícitas sin su *consentimiento*. Un 29 % de las chicas y un 20 % de los chicos han comunicado haber recibido imágenes explícitas *no solicitadas*. La recepción y distribución no deseada de imágenes, incluso cuando no son objetivamente dañinas, ofensivas o vergonzosas, puede afectar al desarrollo de la autoestima, la autonomía y las relaciones del niño, así como a su desarrollo psicosocial”. Asamblea General de las Naciones Unidas, Informe del Relator Especial sobre el derecho a la privacidad, cit., párrafo 89.

⁵⁶ Asamblea General de las Naciones Unidas, Informe del Relator Especial sobre el derecho a la privacidad, cit., párrafo 9. “Con respecto a los niños, las niñas y adolescentes que son lesbianas, gay, bisexuales, trans o intersex (LGBTI), una revisión de evidencia de la UNESCO (2017) encontró que los NNA LGBTI son particularmente más susceptibles a la intimidación y la violencia que los adolescentes que no pertenecen a este colectivo. En la era de Internet, sigue siendo muy frecuente que estos adolescentes también sean víctimas de situaciones de acoso y ciberviolencia y que se enfrenten a la estigmatización y la discriminación en los espacios virtuales por su orientación sexual”. Organización de los Estados Americanos (OEA), Instituto Interamericano del Niño, la Niña y los Adolescentes, Informe regional, cit., 67.

⁵⁷ “Bajo el entendido que el consentimiento deriva del concepto de autonomía y libertad, se entiende que puede ser revocado por cualquier motivo, sin que ello entrañe desventaja o perjuicio alguno, incluso sólo de manera verbal, ya que no es definitivo”. Corte IDH, Caso I. V. vs. Bolivia, Sentencia de 30 de noviembre de 2016, Fondo, Reparaciones y Costas, Serie C, No. 325, párr. 184, <https://jurisprudencia.corteidh.or.cr/es/vid/883974476>

⁵⁸ “La Corte reitera que no basta que los Estados se abstengan de violar los derechos, sino que es imperativa la adopción de medidas positivas, determinables en función de las particulares necesidades de protección del sujeto de derecho, ya sea por su condición personal o por la situación específica en que se encuentre”. Corte IDH, Caso I. V. vs. Bolivia, cit., párrafo 206. En el mismo sentido, conviene observar que, para asegurar, en la mayor medida posible, la prevalencia del interés superior del niño, el preámbulo de la Convención sobre los Derechos del Niño establece que este requiere “cuidados especiales”, y el artículo 19 de la Convención Americana sobre Derechos Humanos (CADH), señala que debe recibir “medidas especiales de protección”. Corte IDH, Caso Gonzales Lluy y otros vs. Ecuador, Sentencia de 1 de septiembre de 2015, Fondo, Reparaciones y Costas, Serie C, No. 298, párrafo 268, https://www.corteidh.or.cr/docs/casos/articulos/seriec_298_esp.pdf

modo que se garantice “su vida, supervivencia y desarrollo”,⁵⁹ así como su facultad de autodeterminación informativa en sintonía con la CDN.⁶⁰

Más significativamente, en el Caso Miembros de la Corporación Colectivo de Abogados “José Alvear Restrepo” vs. Colombia (2023), la Corte IDH reconoció por vez primera el derecho a la autodeterminación informativa como categoría autónoma protegida por la Convención Americana sobre Derechos Humanos (CADH), definiendo su contenido esencial como “la facultad de acceder y controlar los datos de carácter personal en poder de todo órgano público y [...] de particulares”,⁶¹ pudiendo operar, a través del contenido tutelar de los artículos 11 y 13 de la Convención, “como garantía para el ejercicio de otros derechos como la privacidad, la honra, el acceso a la información [...] y en general, la dignidad de las personas”.⁶² Adicionalmente, la Corte IDH sostuvo que la protección de datos personales exige que la recolección, almacenamiento, tratamiento y difusión de información personal “se lleve a cabo solamente en virtud del consentimiento libre e informado del titular de los datos o de un marco normativo que lo autorice”.⁶³

Estos precedentes permiten amplificar, en suma, el *corpus iuris* interamericano en materia de privacidad hacia el concepto de soberanía informacional, esto es, el derecho a controlar el ciclo de vida de los datos personales –desde su recopilación hasta su supresión– en condiciones que no dependan del arbitrio de los adultos ni de cláusulas ininteligibles, sino de marcos normativos deliberativos y evolutivamente adecuados conforme al estándar universal de “adquisición gradual de competencias”.⁶⁴

⁵⁹ Corte IDH, Opinión Consultiva OC-21/14 de 19 de agosto de 2014, Derechos y garantías de niñas y niños en el contexto de la migración y/o en necesidad de protección internacional, solicitada por las Repúblicas de Argentina, Brasil, Paraguay y Uruguay, Serie A, No. 21, párrafo 103, https://www.corteidh.or.cr/docs/opiniones/seriea_21_esp.pdf

⁶⁰ En el mismo sentido, ver Corte IDH, Opinión Consultiva OC-17/2002 de 28 de agosto de 2002, Condición Jurídica y Derechos Humanos del Niño, solicitada por la Comisión Interamericana de Derechos Humanos, Serie A, No. 17, párrafo 41, https://www.corteidh.or.cr/docs/opiniones/seriea_17_esp.pdf

⁶¹ Corte IDH, Caso Miembros de la Corporación Colectivo de Abogados “José Alvear Restrepo” vs. Colombia, Sentencia de 18 de octubre de 2023, Fondo, Reparaciones y Costas, Serie C, No. 506, párrafo 585, https://www.corteidh.or.cr/docs/casos/articulos/seriec_506_esp.pdf

⁶² Corte IDH, Caso Miembros de la Corporación de Abogados “José Alvear Restrepo” vs. Colombia, cit., párrafo 588.

⁶³ Corte IDH, Caso Miembros de la Corporación de Abogados “José Alvear Restrepo” vs. Colombia, cit., párrafo 573.

⁶⁴ CDN, Observación General No. 25, cit., párrafo 19. A pesar de estas directivas, Coffe sostiene: “Las mejoras introducidas en las disposiciones relativas al consentimiento encuentran un límite, dado que los patrones oscuros (*dark patterns*) no constituyen sino una manifestación específica de un problema más amplio: el poder de manipulación. [...] Sin embargo, el derecho vigente permanece ajeno a la manipulación, en la medida en que se sustenta en el mito de la racionalidad —esto es, la idea de que somos inmunes a ella— y en el mito de la apatía —la creencia de que, si “elegimos” reducir nuestra privacidad, ello implica

4. La debida diligencia empresarial y la dimensión ética en la arquitectura digital contemporánea: experiencias comparadas y el caso boliviano

En el marco de la progresiva digitalización de la vida social y la consolidación de nuevas formas de gobernanza algorítmica, surge la necesidad de adoptar una *ética pública digital* sustentada en estándares internacionales de derechos humanos. Este giro normativo –caracterizado por una ampliación sustantiva de las obligaciones positivas de los Estados y los deberes de debida diligencia empresarial– ha sido recogido en documentos paradigmáticos como la OG-16 del Comité DN, misma que exige, en consonancia con el principio de “*protection by design and by default*” consagrado en el Reglamento General de Protección de Datos (RGPD) europeo (art. 25),⁶⁵ una transformación estructural en la forma en que se diseñan, implementan y evalúan las tecnologías digitales que afectan a NNA.

En esa misma línea, resulta de singular importancia la iniciativa del Instituto de Investigación de Datos y Sociedad (IIDS) del Uruguay, que en 2018 propuso la incorporación de criterios derivados del *corpus iuris* internacional de los derechos humanos como parte integrante del ciclo de vida de los sistemas de inteligencia artificial (SIA). El documento plantea que la cooperación estructurada entre actores empresariales, organizaciones de derechos civiles y académicos expertos debe institucionalizarse a través de mecanismos de evaluación de impacto en derechos humanos –equivalente funcional de las evaluaciones de impacto de protección de datos previstas por el RGPD (art. 35)⁶⁶ y, en el ámbito de la infancia, por la OG-16 arriba descrita–⁶⁷ como condición ineludible de legitimidad y responsabilidad democrática.⁶⁸

Esta arquitectura regulatoria encuentra respaldo, asimismo, en la OG-25 del Comité DN, cuyo sustrato subraya el deber de los Estados de garantizar que los

necesariamente que estamos conformes con dicha decisión—. La manipulación provoca que incluso disposiciones reforzadas en materia de consentimiento, frecuentemente celebradas como mejores prácticas, tales como el consentimiento expreso (*opt-in*) y el consentimiento informado, resulten ineficaces para protegernos.” (Traducción propia). Cofone, *The Privacy Fallacy...*, cap. 4 (*Manipulation by Design*).

⁶⁵ Parlamento Europeo y Consejo de la Unión Europea, Reglamento (UE) 2016/679, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), 27 de abril de 2016, *Diario Oficial de la Unión Europea* L19 (4 de mayo de 2016), artículo 25 (Protección de datos desde el diseño y por defecto), <https://www.boe.es/doue/2016/119/L00001-00088.pdf>

⁶⁶ Parlamento Europeo y Consejo de la Unión Europea, Reglamento (UE) 2016/679, cit., artículo 35 (Evaluación de impacto relativa a la protección de datos).

⁶⁷ CDN, Observación General No. 16, cit., párrafos 78-81.

⁶⁸ Karen Hao, “La falta de ética de la IA amenaza con destruir la justicia social”, *MIT Technology Review* (2018), <https://www.technologyreview.es/s/10623/la-falta-de-etica-de-la-ia-amenaza-con-destruir-la-justicia-social>

proveedores de servicios digitales no solo apliquen salvaguardias idóneas, sino que lo hagan articulando mecanismos de participación efectiva de la infancia en el diseño mismo de sus entornos digitales.⁶⁹ Esta formulación converge con la exigencia contenida en el artículo 25 del RGPD europeo, al establecer que la privacidad y la protección de datos personales deben ser integradas *ex ante* en los procesos tecnológicos como diseño estructurante, y no como reacción formal *ex post*.⁷⁰

Complementariamente, los Principios Empresariales sobre los Derechos del Niño, desarrollados por el Pacto Mundial de las Naciones Unidas y Save the Children, articulan una concepción robusta de la diligencia debida, obligando a las corporaciones a prevenir, mitigar y remediar los impactos adversos –reales o potenciales– que sus operaciones generen sobre la infancia.⁷¹ Sin embargo, la región latinoamericana presenta un escenario deficitario en cuanto concierne a validez y eficacia normativa. Tal es el caso de México, donde la Ley Federal de Telecomunicaciones y Radiodifusión permite a las autoridades acceder, sin orden judicial previa, a la geolocalización en tiempo real de los usuarios, vulnerando así una serie de principios esenciales relativos a la necesidad, proporcionalidad e idoneidad en lo atinente al tratamiento de datos personales.⁷²

En Bolivia, esta problemática adquiere especial relevancia. A pesar del reconocimiento constitucional que ha adquirido el derecho a la privacidad⁷³ y, en la esfera jurisprudencial, el derecho a la *autodeterminación informativa* –entendido como la “potestad o facultad que tiene toda persona de disponer de la información o de los datos personales concernientes a su personalidad”,⁷⁴ cuyo ámbito tutelar comprende aquellos datos que son compilados, almacenados y utilizados a través de las plataformas comunicacionales–,⁷⁵ subsisten interpretaciones gubernamentales que

⁶⁹ CDN, Observación General No. 25, cit., párrafo 17.

⁷⁰ Parlamento Europeo y Consejo de la Unión Europea, Reglamento (UE) 2016/679, cit., artículo 25 (Protección de datos desde el diseño y por defecto).

⁷¹ Unicef y Save the Children, *Derechos del niño y principios empresariales*, 25 de junio de 2014, <https://www.unicef.org/lac/media/6791/file/PDF%20Derechos%20del%20ni%C3%B1o%20y%20principios%20empresariales.pdf>. En sentido similar, ver Observación General No. 16, cit., párrafos 62-65.

⁷² Mucio Israel Hernández Guerrero, “Privacidad y datos personales en internet”, *Revista de Derechos Humanos XIV*, n.º 6 (2016): 25.

⁷³ Art. 21: “Las bolivianas y los bolivianos tienen los siguientes derechos: (...) 2. A la privacidad, intimidad, honra, honor, propia imagen y dignidad”. Constitución Política del Estado Plurinacional de Bolivia, promulgada el 7 de febrero de 2009, *Gaceta Oficial del Estado Plurinacional de Bolivia*, <https://www.gacetaoficialdebolivia.gob.bo/normas/view/45387>

⁷⁴ Tribunal Constitucional Plurinacional de Bolivia (TCP), Sentencia Constitucional Plurinacional 0041/2025-S3 de 10 de marzo de 2025, Expediente 69797-2024-140-APP.

⁷⁵ “En ese sentido y considerando que la propagación de datos, sean textos, sonidos o imágenes, se amplifica dentro las redes sociales y en caso de mostrarse de forma negativa puede ser irreparablemente perjudicial para el ejercicio del derecho a la honra asociado a otros como los relativos a la propia imagen y a la intimidad personal y familiar, y sobre todo al concepto de dignidad humana, resulta lógico pensar en una protección constitucional inmediata, siempre

propugnan la “propietarización” de la información personal por parte del Estado.⁷⁶ Esta tesis colisiona no solo con los estándares de derechos humanos arriba expuestos, sino también con el enfoque garantista que trasunta en el RGPD europeo, donde la titularidad de los datos personales es inalienable e indisponible, y su tratamiento debe ajustarse, *inter alia*, a criterios de licitud, lealtad y transparencia (art. 5).⁷⁷

A su vez, diversos informes publicados por organizaciones de la sociedad civil evidencian una ausencia crítica de políticas públicas diferenciadas y adaptadas a las necesidades digitales de la infancia, caracterizadas por una baja transparencia en el uso de algoritmos estatales y prácticas deficientes de protección de datos.⁷⁸ Por ejemplo, el documento de análisis “Privacidad y protección de datos. Propuestas pre-electorales 2024-2025”, elaborado por la Fundación Internet Bolivia, da cuenta de una sistemática opacidad en el tratamiento de información personal por parte de organismos estatales y actores privados, señalando episodios de acoso digital, ciberestafas, divulgación no consentida de datos sensibles, y contacto no autorizado por parte de adultos hacia NNA para fines de explotación sexual o trata.⁷⁹

Esta situación devela fallas críticas en la implementación de principios mínimos de seguridad y transparencia, contraviniendo abiertamente lineamientos marco como aquellos regidos por los artículos 24 y 25 del RGPD, así como las exigencias de “diligencia debida” contenidas en la OG-16 del Comité DN, que obligan a los Estados a “detectar, prevenir y mitigar” los impactos adversos derivados de operaciones digitales sobre poblaciones vulnerables.⁸⁰

En el mismo sentido, el informe elaborado por la Fundación FES-Bolivia ha denunciado la implementación del programa “Yo no soy X” del Órgano Electoral Plurinacional (OEP), en el que se habrían recabado datos biométricos de adolescentes entre 16 y 18 años sin el consentimiento informado y verificable de sus representantes

y cuando exista una deducción incuestionable respecto a la autoría sobre el hecho vulneratorio”. TCP, Sentencia Constitucional Plurinacional 0552/2024-S4 de 2 de septiembre de 2024, Exp. 57759-2023-116-APP, 13. En el mismo sentido, ver TCP, Sentencia Constitucional Plurinacional 0021/2021-S2 de 7 de abril de 2021, Exp. 29264-2019-59-APP.

⁷⁶ Fundación Internet Bolivia, Derechos Digitales y Access Now, “Derechos Humanos en el entorno digital en Bolivia”, Comunicación conjunta presentada en el marco del Examen Periódico Universal, 34° período de sesiones, Estado Plurinacional de Bolivia, marzo de 2019, 8, <https://www.accessnow.org/wp-content/uploads/2019/05/Informe-Partes-Interesadas-derechos-digitales-Bolivia.pdf>

⁷⁷ Parlamento Europeo y Consejo de la Unión Europea, Reglamento (UE) 2016/679, cit., artículo 5 (Principios relativos al tratamiento).

⁷⁸ Fundación Internet Bolivia, Derechos Digitales y Access Now, “Derechos Humanos en el entorno digital en Bolivia”, 13.

⁷⁹ Fundación Internet Bolivia.org, “Privacidad y protección de datos. Propuestas pre-electorales 2024-2025”, Proyecto: Caminos posibles para los derechos digitales en Bolivia, septiembre de 2024, 3 y 6, https://internetbolivia.org/file/2024/11/fdd_03.pdf

⁸⁰ CDN, Observación General No. 16, cit., párrafo 45.

legales.⁸¹ Tal omisión no solo vulnera el derecho a la autodeterminación informativa en su dimensión relacional, sino que erosiona la legitimidad institucional, al desconocer la “capacidad evolutiva” de NNA, principio recogido tanto en la CDN como en la Observación General No. 7 del Comité Africano *ut supra*. La falta de mecanismos adecuados de información previa, y la inexistencia de procedimientos efectivos de auditoría y rendición de cuentas consolidan un entorno de desprotección sistémica en el que la privacidad infantil queda expuesta a un uso instrumental de su identidad digital. Esta acuciante coyuntura pone de relieve la necesidad de adoptar una ley integral de protección de datos personales⁸² en línea con las mejores prácticas del derecho comparado⁸³ y en armonía con los estándares internacionales arriba descritos, que reconozca expresamente la protección reforzada de NNA en entornos digitales conforme al principio de precaución y al “enfoque por defecto” del RGPD, así como los principios de minimización, participación, transparencia y autonomía progresiva.

Cualquier respuesta legislativa eficaz debe evitar la reproducción inercial de marcos normativos que han demostrado limitaciones estructurales. Como advierte Ignacio Cofone, el estándar clásico de consentimiento –como eje legitimador del tratamiento de datos– resulta cada vez más desfasado frente a arquitecturas tecnológicas diseñadas para moldear preferencias y erosionar la agencia individual.⁸⁴ Esta

⁸¹ Fundación Friedrich Ebert Stiftung (Bolivia), Fundación Internet Bolivia.org y Derechos Digitales, “Situación de la privacidad en Bolivia”, Serie FUTURODIGITAL.bo, La Paz: América Latina, febrero de 2020, 26, https://internetbolivia.org/file/2020/05/fd_privacidad_bo_v1.pdf

⁸² En mayo de 2019, y como resultado de “talleres abiertos realizados con ciudadanía y diferentes organizaciones de La Paz, El Alto, Cochabamba y Santa Cruz”, la Fundación Internet Bolivia.org publicó un anteproyecto de “Ley ciudadana de privacidad y protección de datos personales”, cuyo contenido puede revisarse en https://misdatos.internetbolivia.org/docs/anteproyecto_ley_de_proteccion_datos_personales_InternetBolivia.pdf. Tiempo después, en 2023, la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (Agetic), dependiente del Gobierno boliviano, presentó un “Anteproyecto de Ley de Protección de Datos Personales”, cuyo sustrato puede revisarse, asimismo, en <https://www.dataguidance.com/sites/default/files/agetic.pdf>. A pesar de los innegables avances que ambos proyectos comportan, las disposiciones relativas a la protección de las personas menores de edad en los ecosistemas digitales son exiguas –cuando no barrocas– y no incorporan los principios ni estándares diferenciados, tanto internacionales como regionales, ampliamente explicitados *supra*.

⁸³ Ana Torres Menárguez, “La pionera ley australiana que veta a los menores de 16 el acceso a redes sociales”, *El País*, 28 de noviembre de 2024, <https://elpais.com/sociedad/2024-11-28/claves-la-pionera-ley-australiana-que-veta-a-los-menores-de-16-el-acceso-a-redes-sociales.html>; EFE, “Nueva Zelanda plantea prohibir el acceso a las redes a menores de 16 años”, *El País*, 6 de mayo de 2025, <https://elpais.com/sociedad/2025-05-06/nueva-zelanda-plantea-prohibir-el-acceso-a-las-redes-a-menores-de-16-anos.html>

⁸⁴ “Los diseñadores configuran de manera sistemática arquitecturas de elección con el fin de inducir a las personas a aceptar condiciones que benefician a las corporaciones. Así, por ejemplo, pueden respaldar una alternativa y destacar las pérdidas asociadas a la otra, o bien minimizar las preocupaciones relativas a la privacidad, predisponiendo a las personas a otorgar su consentimiento. Muchas empresas utilizan botones de distintos tamaños y colores

perspectiva crítica converge con una creciente literatura que cuestiona los modelos de autodeterminación informativa anclados en supuestos de racionalidad individual, alertando sobre las formas de manipulación estructural que subyacen en los entornos digitales y que afectan con particular intensidad a los sujetos en desarrollo (i. e., NNA), cuya capacidad resolutoria aún se encuentra en formación.

5. A modo de colofón: Por una cultura de la dignidad para la niñez y la adolescencia frente a la cultura de exposición en internet

El análisis desarrollado líneas arriba permite colegir que la expansión sin precedentes de la tecnología digital ha desencadenado un profundo proceso de *datificación* de la existencia, en el que las personas menores de edad se constituyen en uno de los colectivos más expuestos a los riesgos relacionados con los contenidos, los contactos, las conductas y los contratos en los entornos digitales.⁸⁵ La infancia, en su calidad de sujeto constitucional de especial protección, se encuentra inmersa en un entorno tecnológicamente mediado que transforma radicalmente los términos clásicos de la privacidad, el consentimiento y la autonomía individual, exigiendo una relectura sustantiva del marco normativo vigente bajo las coordenadas de la autodeterminación informacional.

En este contexto, resulta ineludible comprender la privacidad no como una dimensión meramente negativa o reactiva del derecho, sino como un poder positivo fundado en la antedicha soberanía informativa, que articula el desarrollo pleno y seguro de la subjetividad infantil. La inferencialidad algorítmica –esto es, la capacidad de las tecnologías actuales para extraer, deducir y manipular rasgos personales sin interacción directa– ha erosionado las bases tradicionales del consentimiento, transfigurándolo en un acto ritual carente de voluntarismo. Esta mutación identitaria impone una arquitectura de garantías centrada en la anticipación, la prevención de daños y la minimización de datos, principios recogidos por el propio RGPD europeo, así como el *corpus iuris* universal e interamericano de derechos humanos mencionados *supra*.

Desde el prisma constitucional, la protección de la infancia frente al poder tecnopolítico no puede descansar exclusivamente en mecanismos procesales *ex post*. Debe afirmarse, *a contrario*, en un constitucionalismo deliberativo que incorpore la noción de consentimiento reforzado, por defecto (*by default*), y evolutivamente apropiado, como expresión de una (nueva) ética pública en clave digital. Ello exige, por un lado, marcos normativos que estructuren legalmente la rendición de cuentas

para aquellas opciones que desean que los usuarios seleccionen. Otras tratan de influir en nuestras decisiones explotando nuestra aversión a las pérdidas” (traducción propia). Cofone, *The Privacy Fallacy*..., 39.

⁸⁵ CDN, Observación General No. 25, cit., párrafo 14.

de las corporaciones digitales y, por otro, acciones afirmativas del Estado orientadas a garantizar el acceso libre, seguro e inclusivo a los ecosistemas digitales a partir de una lógica de justicia intergeneracional y procedimental, donde las personas menores de edad puedan adoptar decisiones informadas.

Las diversas evidencias documentadas en el caso boliviano –como la recolección sin consentimiento de datos biométricos a través del programa “Yo no soy X”, la exposición de NNA a prácticas de acoso, explotación y comercialización de datos sin salvaguardias adecuadas, o la tendencia estatal a “propietarizar” la información personal– revelan un déficit estructural que no puede subsanarse mediante regulaciones inocuas. Lo anterior torna imperativo la adopción de una ley integral de protección de datos personales que reconozca la titularidad inalienable e indisponible de la información privada, con mecanismos eficaces de fiscalización, participación y evaluación de impacto en derechos humanos, especialmente en lo referido a la infancia.

Simultáneamente, debe empezar a construirse –paulatina y articuladamente– una “cultura de la dignidad”, en oposición a la “cultura de exposición” en internet, que materialice las directivas marco desarrolladas por la jurisprudencia constante de la Corte IDH y tribunales regionales. Este giro cualitativo supone repensar el consentimiento, no como un mero “clic” que valida el acceso a contenidos, sino como una *praxis* cognitiva e institucionalmente mediada, capaz de reflejar una comprensión real y una voluntad auténtica por parte de NNA. A ello contribuyen propuestas como la “responsabilidad significativa” (*meaningful accountability*) de Cofone, que aboga por un nuevo tipo de responsabilidad jurídica –basado en el daño intrínseco a la privacidad– que supere la ficción del consentimiento autogestionado, reconociendo la privacidad como un “bien social colectivo” y no como una mera transacción individual.⁸⁶

En definitiva, la defensa de la infancia frente a los riesgos inherentes a la gobernanza algorítmica exige una renovación profunda de las categorías jurídicas, técnicas y éticas que rigen la digitalidad. Una nueva arquitectura de la elección debe asentarse sobre bases normativas robustas, deliberativas y evolutivamente adecuadas, en las que el derecho a la privacidad se configure como la piedra de toque de la ciudadanía digital infantil. Solo de esta manera será posible contrarrestar las dinámicas de vigilancia, manipulación y explotación que hoy amenazan, cual ciberpanóptico orwelliano, a los sujetos más vulnerables en una sociedad cada vez más automatizada.

Bibliografía

DOCTRINA

5RIGHTS FOUNDATION. “A high level of privacy, safety & security for minors: A best practices baseline for the implementation of the Digital Services Act

⁸⁶ Cofone, *The Privacy Fallacy*..., 6; 65-66; 163-164; 138-139.

- for Children”, febrero de 2024. <https://5rightsfoundation.com/wp-content/uploads/2024/08/5rights-foundation-a-high-level-of-privacy-safety-and-security-for-minors-dsa-baseline-2024-final-1.pdf>
- ÁLVAREZ MEDINA, Silvina. “Derechos humanos emergentes: fundamentación, contenido y sujetos desde una perspectiva de género”. En *Repensar los derechos humanos*, editado por Ángeles RÓDENAS. Lima: Palestra Editores, 2018.
- BURGORGUE-LARSEN, Laurence. “Decomartmentalization: The key technique for interpreting regional human rights treaties”. *International Journal of Constitutional Law* 16, n.º 1 (2018): 187-213. <https://doi.org/10.1093/icon/moy010>
- COFONE, Ignacio. *The Privacy Fallacy: Harm and Power in the Information Economy*. Cambridge: Cambridge University Press, 2024.
- DJEFFAL, Christian. “Children’s Rights by Design and Internet Governance: Revisiting General Comment No. 25 (2021) on Children’s Rights in Relation to the Digital Environment”. *Laws* 11, n.º 4 (2022). <https://doi.org/10.3390/laws11040084>
- ENEYEW AYALEW, Yohannes, Valerie VERDOODT y Eva LIEVENS. “General Comment No. 25 on Children’s Rights in Relation to the Digital Environment: Implications for Children’s Right to Privacy and Data Protection in Africa”. *Human Rights Law Review* 24, n.º 3 (2024). <https://doi.org/10.1093/hrlr/ngae018>
- FOSCH-VILLARONGA, Eduard et al. *The Chilling Effects of Algorithmic Profiling and Automated Decision-Making*. eLaw Working Paper Series. Leiden: Universiteit Leiden, 2020. <https://www.universiteitleiden.nl/binaries/content/assets/rechtsgeleerdheid/instituut-voor-metajuridica/elaw-working-paper-series/wps2020.001.fosch.the-chilling-effects-of-algorithmic.pdf>
- FUNDACIÓN INTERNET BOLIVIA.org. “Privacidad y protección de datos. Propuestas pre-electorales 2024-2025”. Proyecto: Caminos posibles para los derechos digitales en Bolivia, septiembre de 2024.
- GARCÍA PACHÓN, María del Pilar, ed. *Información, participación y justicia ambiental: herramientas para alcanzar el desarrollo sostenible en la democracia ambiental*. Bogotá: Universidad Externado de Colombia, 2020.
- HAO, Karen. “La falta de ética de la IA amenaza con destruir la justicia social”. *MIT Technology Review*, 2018. <https://www.technologyreview.es/s/10623/la-falta-de-etica-de-la-ia-amenaza-con-destruir-la-justicia-social>
- HERNÁNDEZ GUERRERO, Mucio Israel. “Privacidad y datos personales en internet”. *Revista de Derechos Humanos XIV*, n.º 6 (2016).
- LASSALLE, José María. *Ciberleviatán. El colapso de la democracia liberal frente a la revolución digital*. Barcelona: Arpa Editores, 2019.
- LASSALLE, José María. *Civilización artificial*. Barcelona: Arpa Editores, 2024.
- MAI, Jens-Erik. “Situating personal information: Privacy in the algorithmic age”. En *Human Rights in the Age of Platforms*, editado por Rikke Frank JØRGENSEN, 79-98. Cambridge, MA: MIT Press, 2019.
- NIÑO GONZÁLEZ, José Ignacio, Mario BARQUERO CABRERO y Enrique GARCÍA GARCÍA. “Opinión pública e infoxicación en las redes: los fundamentos de la

- post-verdad". *Vivat Academia* 139 (2017): 83-94. <https://www.redalyc.org/journal/5257/525754431007/html/>
- NISSENBAUM, Helen. "Privacy as contextual integrity". *Washington Law Review* 79 (2004): 119-158. <https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10>
- ORGANIZACIÓN DE LOS ESTADOS AMERICANOS (OEA), Instituto Interamericano del Niño, la Niña y los Adolescentes. Informe regional: "Lineamientos para el empoderamiento y la protección de los derechos de los niños, niñas y adolescentes en Internet en Centroamérica y República Dominicana". OEA/Ser.D/XX-VI.18, enero de 2018. <https://www.oas.org/es/sadye/publicaciones/InfRegional-ESP008-WEB.pdf>
- RAWLS, John. *Teoría de la justicia*, 2.^a ed. México D. F.: Fondo de Cultura Económica, 2006.
- RIVOIR, Ana y Susana LAMSCHEIN. "Plan Ceibal, un caso de usos de las tecnologías de información y de las comunicaciones en la educación para la inclusión social". En *Las tecnologías digitales frente a los desafíos de una educación inclusiva en América Latina: Algunos casos de buenas prácticas*, editado por Guillermo SUNKEL y Daniela TRUCCO, 155-180. Santiago de Chile: Comisión Económica para América Latina y el Caribe, 2012. <https://repositorio.cepal.org/server/api/core/bitstreams/7be78858-1bdf-4c59-b7d2-78532198900b/content>
- SPECTOR, Ezequiel. *La libertad entendida como cooperación social. Una teoría de la democracia liberal*. Barcelona: Marcial Pons, 2025.
- VÉLIZ, Carissa. *Privacidad es poder: datos, vigilancia y libertad en la era digital*. Barcelona: Debate, 2020.
- ZUBOFF, Shoshanna. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs, 2019.

NORMATIVA Y JURISPRUDENCIA

- AFRICAN COMMITTEE OF EXPERTS ON THE RIGHTS AND WELFARE OF THE CHILD. General Comment No. 7 on Article 27 of the ACRWC: "Sexual Exploitation", 21 de julio de 2022. https://reporting.acerwc.africa/sites/default/files/2022-09/General-Comment-on-Article-27-of-the-ACRWC_English_o.pdf
- COMITÉ DE LOS DERECHOS DEL NIÑO. Observación General No. 16 de 17 de abril de 2013 sobre las obligaciones del Estado en relación con el impacto del sector empresarial en los derechos del niño. Naciones Unidas, CRC/C/GC/16. <https://www.plataformadeinfancia.org/wp-content/uploads/2018/09/observacion-general-16-obligaciones-estado-relacion-con-impacto-sector-empresarial-derechos-nino-2013-.pdf>
- COMITÉ DE LOS DERECHOS DEL NIÑO. Observación General No. 25 de 2 de marzo de 2021. Los derechos de los niños en relación a los entornos digitales. Naciones Unidas, CRC/C/GC/25. <https://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPRiCAqhKb7yhsqIkirKQZLK2M58RF%2F5FovEG%2F>

2BcAAx34gC78FwvnmZXGFO6kxoVqQk6dNAzTPSRNxomyCaUSrDC%2Fod3UDPTV4y05%2B9GMEoqMZvh9UPKTXcO12

CONSEJO DE EUROPA. “La dimensión digital de la violencia contra la mujer abordada por los siete mecanismos de la Plataforma EDVAW”. Documento temático de la Plataforma de Mecanismos de Expertos Independientes sobre la Discriminación y la Violencia contra la Mujer, EDVAW, noviembre de 2022. <https://rm.coe.int/la-dimension-digital-de-la-violencia-contra-la-mujer-abordada-por-los-/1680a933ad>

CONSTITUTIONAL COURT OF SOUTH AFRICA. Centre for Child Law and Others v Media 24 Limited and Others. Sentencia de 4 de diciembre de 2019. ZACC 46. <https://www.saflii.org/za/cases/ZACC/2019/46.html>

CORTE INTERAMERICANA DE DERECHOS HUMANOS (CORTE IDH). Caso Fonteviechia y D’Amico vs. Argentina. Sentencia de 29 de noviembre de 2011. Fondo, Reparaciones y Costas. Serie C, No. 238. https://corteidh.or.cr/docs/casos/articulos/seriec_238_esp.pdf

CORTE IDH. Caso Artavia Murillo y otros (“Fecundación *in vitro*”) vs. Costa Rica. Sentencia de 28 de noviembre de 2012. Excepciones Preliminares, Fondo, Reparaciones y Costas. Serie C, No. 257. https://www.corteidh.or.cr/docs/casos/articulos/seriec_257_esp.pdf

CORTE IDH. Caso Gonzales Lluy y otros vs. Ecuador. Sentencia de 1 de septiembre de 2015. Fondo, Reparaciones y Costas. Serie C, núm. 298. https://www.corteidh.or.cr/docs/casos/articulos/seriec_298_esp.pdf

CORTE IDH. Caso I. V. vs. Bolivia. Sentencia de 30 de noviembre de 2016. Fondo, Reparaciones y Costas. Serie C, No. 329. https://www.corteidh.or.cr/docs/casos/articulos/seriec_329_esp.pdf

CORTE IDH. Caso Miembros de la Corporación Colectivo de Abogados “José Alvear Restrepo” vs. Colombia. Sentencia de 18 de octubre de 2023. Fondo, Reparaciones y Costas. Serie C, núm. 506. https://www.corteidh.or.cr/docs/casos/articulos/seriec_506_esp.pdf

CORTE IDH. Opinión Consultiva OC-17/2002 de 28 de agosto de 2002. Condición Jurídica y Derechos Humanos del Niño. Solicitada por la Comisión Interamericana de Derechos Humanos. Serie A, No. 17. https://www.corteidh.or.cr/docs/opiniones/seriea_17_esp.pdf

CORTE IDH. Opinión Consultiva OC-21/14 de 19 de agosto de 2014. Derechos y garantías de niñas y niños en el contexto de la migración y/o en necesidad de protección internacional. Solicitada por la República Argentina, la República Federativa de Brasil, la República del Paraguay y la República Oriental del Uruguay. Serie A, No. 21. https://www.corteidh.or.cr/docs/opiniones/seriea_21_esp.pdf

ESTADO PLURINACIONAL DE BOLIVIA. Constitución Política del Estado Plurinacional de Bolivia. Promulgada el 7 de febrero de 2009. *Gaceta Oficial del Estado Plurinacional de Bolivia*, 003. <https://www.gacetaoficialdebolivia.gob.bo/normas/view/45387>

- EUROPEAN COMMISSION. *Incels: A First Scan of the Phenomenon (in the EU) and its Relevance and Challenges for P/CVE*. Luxembourg: Publications Office of the European Union, 2021. https://home-affairs.ec.europa.eu/system/files/2021-10/ran_incels_first_scan_of_phenomen_and_relevance_challenges_for_p-cve_202110_en.pdf
- ORGANIZACIÓN DE LAS NACIONES UNIDAS (ONU), ASAMBLEA GENERAL. Convención sobre los Derechos del Niño. Resolución 44/25 de 20 de noviembre de 1989. United Nations Treaty Series, vol. 1577. <https://www.refworld.org/es/leg/trat/agonu/1989/es/18815>
- ONU, ASAMBLEA GENERAL, CONSEJO DE DERECHOS HUMANOS. Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, Frank La Rue. A/HRC/23/40, 17 de abril de 2013.
- ONU, ASAMBLEA GENERAL. Informe del Relator Especial sobre el derecho a la privacidad, Joseph A. Cannataci. Derecho a la privacidad. A/76/220, 23 de julio de 2021. <https://documents.un.org/doc/undoc/gen/n21/203/69/pdf/n2120369.pdf>
- ORGANIZACIÓN DE LOS ESTADOS AMERICANOS (OEA), Comité Jurídico Interamericano (CJI). Principios actualizados sobre la privacidad y la protección de datos personales. Principio tres (Necesidad y proporcionalidad). OEA/Ser.D/XIX.20, diciembre de 2021. <https://www.oas.org/ext/DesktopModules/MVC/OASDnn-Modules/Views/Item/Download.aspx?type=1&id=1185&lang=2>
- OEA, COMISIÓN INTERAMERICANA DE MUJERES (CIM). *La violencia de género en línea contra las mujeres y niñas: Guía de conceptos básicos, herramientas de seguridad digital y estrategias de respuesta*. OEA/Ser.D/XXV.25. <https://www.oas.org/es/cim/docs/ViolenciaGeneroLineaGUIA-ES.pdf>
- PARLAMENTO EUROPEO Y CONSEJO DE LA UNIÓN EUROPEA. Reglamento (UE) 2016/679, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). *Diario Oficial de la Unión Europea* L119, 4 de mayo de 2016. <https://www.boe.es/doue/2016/119/L00001-00088.pdf>
- TRIBUNAL CONSTITUCIONAL PLURINACIONAL DE BOLIVIA. Sentencia Constitucional Plurinacional 0021/2021-S2 de 7 de abril de 2021. Expediente 29264-2019-59-APP.
- TRIBUNAL CONSTITUCIONAL PLURINACIONAL DE BOLIVIA. Sentencia Constitucional Plurinacional 0552/2024-S4 de 2 de septiembre de 2024. Expediente 57759-2023-116-APP.
- TRIBUNAL CONSTITUCIONAL PLURINACIONAL DE BOLIVIA. Sentencia Constitucional Plurinacional 0041/2025-S3 de 10 de marzo de 2025. Expediente 69797-2024-140-APP.
- TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA. *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others*. Sentencia de 8 de abril de 2014. Asunto C-293/12. <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:62012CJ0293>

TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA. Eva Glawischnig-Piesczek contra Facebook Ireland Limited. Sentencia de 3 de octubre de 2019. Asunto C-18/18. <https://curia.europa.eu/juris/document/document.jsf?text=&docid=218621>

UNICEF Y SAVE THE CHILDREN. *Derechos del niño y principios empresariales*, 25 de junio de 2014. <https://www.unicef.org/lac/media/6791/file/PDF%20Derechos%20del%20ni%C3%B1o%20y%20principios%20empresariales.pdf>

UNITED NATIONS GENERAL ASSEMBLY. Resolution on the Right to Privacy in the Digital Age. A/RES/73/179. December 17, 2018. https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/73/179