**Universidad Andina Simón Bolívar**

**Sede Ecuador**

**Área de Derecho**

Maestría Profesional en Derechos Humanos

Mención en Exigibilidad Estratégica

# La protección de datos personales en el entorno digital y su impacto en el derecho a la salud mental de niños, niñas y adolescentes en Ecuador, período 2020-2024

Víctor Daniel Espinosa Mogrovejo

Tutor: Luis Fernando Enríquez Álvarez

Quito, 2025

# Cláusula de cesión de derecho de publicación

Yo, Víctor Daniel Espinosa Mogrovejo, autor de la tesis intitulada "La Protección de Datos Personales en el Entorno Digital y su Impacto en el Derecho a la Salud Mental de Niños, Niñas y Adolescentes en Ecuador, período 2020-2024", mediante el presente documento dejo constancia de que la obra es de mi exclusiva autoría y producción, que la he elaborado para cumplir con uno de los requisitos previos para la obtención del título de Magíster en Derechos Humanos, Mención en Exigibilidad Estratégica en la Universidad Andina Simón Bolívar, Sede Ecuador.

1. Cedo a la Universidad Andina Simón Bolívar, Sede Ecuador, los derechos exclusivos de reproducción, comunicación pública, distribución y divulgación, durante 36 meses a partir de mi graduación, pudiendo por lo tanto la Universidad, utilizar y usar esta obra por cualquier medio conocido o por conocer, siempre y cuando no se lo haga para obtener beneficio económico. Esta autorización incluye la reproducción total o parcial en los formatos virtual, electrónico, digital, óptico, como usos en red local y en Internet.
2. Declaro que, en caso de presentarse cualquier reclamación de parte de terceros respecto de los derechos de autor/a de la obra antes referida, yo asumiré toda responsabilidad frente a terceros y a la Universidad.
3. En esta fecha entrego a la Secretaría General, el ejemplar respectivo y sus anexos en formato impreso y digital o electrónico.

17 de junio de 2025

Firma:

# Resumen

Este estudio multidisciplinario con enfoque en derechos humanos analiza el derecho a la protección de datos personales y su impacto en la salud mental de niños, niñas y adolescentes en el Ecuador. A través de una metodología cualitativa y descriptiva, se examinan críticamente las dinámicas de extracción y explotación de datos en el entorno digital, identificando los riesgos asociados al modelo de negocios de las grandes plataformas tecnológicas. Se desarrolla un marco conceptual y normativo que abarca estándares internacionales, regionales y nacionales de protección de datos personales, con énfasis en su relación con el derecho a la salud mental de niños, niñas y adolescentes. Los resultados evidencian un marcado desequilibrio de poder entre las empresas de *big data* y los usuario/as, lo que agrava la vulnerabilidad de la niñez y adolescencia frente a prácticas de vigilancia y manipulación digital. Ante esta problemática, se plantea la necesidad de aplicar estrategias de exigibilidad de derechos, combinando litigio estratégico, movilización social, cooperación internacional y mecanismos de corrección. De esta manera, se visibilizan las relaciones conflictivas de poder y se proponen alternativas para garantizar el derecho a la salud mental de la niñez y adolescencia a través de una protección efectiva de sus datos personales en el entorno digital.

Palabras clave: privacidad, protección de datos personales, derecho a la salud mental, entorno digital, niños, niñas y adolescentes, exigibilidad social, política, jurídica e internacional.

Para el Cacas,

el mejor gato del mundo,

un verdadero tipazo que llegó a mi vida por casualidad, pero se quedó para siempre en mi corazón.

Sigues vivo en mis recuerdos. Este trabajo es un reflejo de todo lo que aprendí y viví mientras compartíamos este camino. Te dedico esta etapa como un tributo al amor incondicional que siempre me diste.

Tu luz no la apaga ni la muerte.

Te extrañaré toda la vida.

# Agradecimientos

Quiero expresar mi más profundo agradecimiento a mis padres y a mi abuela. A pesar de la distancia que nos separa, su apoyo incondicional siempre ha estado presente, haciéndome sentir su cercanía en los momentos más desafiantes de esta maestría.

Gracias por su sacrificio, por contribuir económicamente para que pudiera cumplir este sueño y por ser una fuente constante de aliento. Este logro no habría sido posible sin su amor, confianza y las palabras de ánimo que me recordaban que están conmigo, que siempre lo están. Este triunfo también es de ustedes.

# Tabla de contenidos

# Siglas, acrónimos y abreviaturas

| | |
|---|---|
| AN | Asamblea Nacional |
| APC | Association for Progressive Communications |
| CAD | Centro de Autonomía Digital |
| CADH | Convención Americana sobre Derechos Humanos |
| CDH | Comité de Derechos Humanos |
| CEPD | Comité Europeo de Protección de Datos |
| CIDH | Comisión Interamericana de Derechos Humanos |
| CPCCS | Consejo de Participación Ciudadana y Control Social |
| COIP | Código Orgánico Integral Penal |
| COPPINA | Código Orgánico para la Protección Integral de Niños, Niñas y Adolescentes |
| CORDICOM | Consejo de Regulación y Desarrollo de la Información y Comunicación |
| CorteIDH | Corte Interamericana de Derechos Humanos |
| Directrices WP248 | Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento "entraña probablemente un alto riesgo" a efectos del Reglamento (UE) 2016/679 |
| DPO | Delegado de Protección de Datos |
| ENEMDU | Encuesta Nacional de Empleo, Desempleo y Subempleo |
| EPU | Examen Periódico Universal |
| INEC | Instituto Nacional de Estadística y Censos |
| LOFL | Ley Orgánica de la Función Legislativa |
| LOPDP | Ley Orgánica de Protección de Datos Personales |
| LOTDA | Ley Orgánica para la Transformación Digital y Audiovisual |
| NNA | Niños, Niñas y Adolescentes |
| OACDH | Oficina del Alto Comisionado para los Derechos Humanos |
| OEA | Organización de Estados Americanos |
| OG | Observación General |
| PIDCP | Pacto Internacional de Derechos Civiles y Políticos |
| PIDESC | Pacto Internacional de Derechos Económicos, Sociales y Culturales |

| | |
|---|---|
| RGPD | Reglamento General de Protección de Datos |
| RIPD | Red Iberoamericana de Protección de Datos |
| SIDH | Sistema Interamericano de Protección de los Derechos Humanos |
| UE | Unión Europea |

# Introducción

Hoy todo son ordenadores y más ordenadores
Y pronto todo el mundo tendrá uno,
Los niños de tres años tendrán ordenadores
Y todo el mundo conocerá todo
Lo relacionado con los demás
Mucho antes que lleguen a conocerse
Y por eso nadie querrá conocerse.
Nadie querrá conocer a nadie
Nunca jamás
Y todos serán
Unos solitarios
Como lo soy yo hoy.
(Charles Bukowski)

La pandemia evidenció la profunda dependencia de la humanidad hacia Internet como herramienta esencial para la comunicación, el aprendizaje y la interacción social. Si bien el entorno digital ha traído innumerables beneficios, también plantea riesgos significativos para la salud mental de niños, niñas y adolescentes. En Ecuador, este grupo es considerado jurídicamente como incapaz absoluto o relativo, dependiendo de la edad, lo que resalta la vulnerabilidad de su información en el ecosistema digital. Al no contar con plena autonomía para gestionar sus datos, quedan expuestos a prácticas de explotación económica y manipulación algorítmica, afectando su bienestar psicológico.[1]

El crecimiento sostenido de la conectividad en el país, que pasó de una penetración del 45,5 % en 2019 a un 83,6 % en 2024, ha sido acompañado por un aumento de la tasa de uso efectivo de Internet entre niños, niñas y adolescentes (NNA), con un 64,4 % de acceso en hogares y un 69,7 % de usuarios en total.[2] Este fenómeno ha generado un entorno digital en el que los NNA están constantemente expuestos a la recolección de datos por parte de plataformas que priorizan la maximización de la atención sobre la seguridad y bienestar de sus usuarios y usuarias. La brecha generacional y digital entre adultos y NNA, así como la ausencia de una regulación robusta sobre el tratamiento de

[1] The Social Dilemma, “Digital Rights are Human Rights”, *The Social Dilemma,* accedido 16 de septiembre de 2020, párr. 2, https://thedigitalrightsdilemma.splashthat.com.

[2] INEC, encuesta ENEDMU, 2023; INEC Ecuador, "Desigualdades Educativas en el contexto de la pandemia de la COVID-19 en el Ecuador", junio de 2022,https://www.ecuadorencifras.gob.ec/documentos/webinec/Bibliotecas/Libros/Reportes/Educacion_COVID.pdf; "Digital 2024: Ecuador", DataReportal – Global Digital Insights, 23 de febrero de 2024, https://datareportal.com/reports/digital-2024-ecuador.

sus datos personales, agravan la situación, impidiendo una protección integral de sus derechos.

Si bien Ecuador cuenta con la Ley Orgánica de Protección de Datos Personales (LOPDP) y la Ley Orgánica de Salud Mental (LOSM), ambas operan de manera aislada, sin una articulación efectiva para garantizar la protección de la salud mental de los menores en el entorno digital. La vulneración de derechos en este contexto se vuelve tanto una problemática generalizada (por su extensión y repetición en el país)[3] como estructural, dado que se relaciona con el orden político, económico y la concentración del poder en plataformas digitales.[4] Así, en esta investigación se analiza este fenómeno bajo un enfoque crítico de derechos humanos, en la que se busca responder la interrogante: ¿Cómo incide la protección de datos personales en el entorno digital en el pleno ejercicio del derecho a la salud mental de niños, niñas y adolescentes en Ecuador?

Para abordar esta interrogante, el estudio establece tres objetivos principales: conocer la situación actual sobre la protección de datos personales y la salud mental de niños, niñas y adolescentes en el entorno digital; determinar el impacto que dicho entorno ejerce sobre su derecho a la salud mental; y proponer mecanismos de exigibilidad que permitan garantizar su bienestar en el ámbito digital.

El estudio adopta un enfoque cualitativo exploratorio y crítico de derechos humanos, priorizando la comprensión profunda de la relación entre el entorno digital y la salud mental de NNA. La metodología empleada combina entrevistas semiestructuradas con expertos y un análisis documental exhaustivo, lo que permite contrastar percepciones con el marco normativo vigente. Se realizaron entrevistas con nueve informantes clave (cuatro psicólogos, cuatro expertos en protección de datos y una usuaria de la plataforma *Worldcoin*) seleccionados mediante criterios de diversidad de género, experiencia en salud mental y protección de datos, y disponibilidad para participar entre mayo y junio de 2024. Adicionalmente, el análisis documental incluyó textos legales, resoluciones judiciales y estudios académicos.

[3] Una violación de derechos humanos es generalizada cuando existe un alto número de casos, se practica de forma extendida en un territorio determinado se realiza en un marco de impunidad. En Flacso, "Violaciones, derechos humanos y contexto: herramientas propuestas para documentar e investigar. Manual de Análisis de Contexto para Casos de Violaciones a los Derechos Humanos" (International Bar Association's Human Rights Institute, 2017), 43.

[4] Una vulneración de derechos humanos es estructural cuando está relacionada con el orden político, económico y con los procesos de concentración del poder, así como de construcción de la cultura política. Ibíd., 45.

El procesamiento de la información se llevó a cabo mediante la transcripción de entrevistas, luego se empleó codificación abierta para extraer conceptos emergentes de cada entrevista, seguida de codificación axial para agruparlos temáticamente, y finalmente se contrastaron estos hallazgos con el análisis documental para garantizar coherencia y validez interna del estudio. Los resultados fueron organizados en cinco categorías operativas: impacto en la salud mental (sexualización, ansiedad, depresión, hiperconsumo, violencia digital e hiperconectividad), pandemia y virtualidad (transformaciones en educación, salud emocional y brecha digital), corresponsabilidad (rol de familia, Estado y empresas tecnológicas), protección de datos personales (riesgos en redes, cumplimiento normativo e instituciones supervisoras) y alternativas (propuestas de cooperación internacional y enfoques integrales para mejorar la protección de derechos en entornos digitales).

Todos los participantes otorgaron su consentimiento informado,[5] garantizando el anonimato del testimonio de la presunta víctima y el respeto a los principios éticos de la investigación. Se procuró preservar la fidelidad de los relatos sin interpretaciones sesgadas, protegiendo la identidad de los participantes y evitando el uso de datos personales fuera del contexto de estudio.

El primer capítulo analiza cómo el big data y los algoritmos, en el marco del capitalismo de la vigilancia, han convertido los datos personales en mercancías, condicionando la voluntad individual y vulnerando principios como la dignidad y la autodeterminación informativa. Examina el contenido y alcance del derecho a la protección de datos personales desde marcos internacionales y nacionales, comparando la norma ecuatoriana con el Reglamento General de la UE, y destacando la importancia de la gestión de riesgos y la responsabilidad proactiva. Además, aborda la salud mental de niños, niñas y adolescentes en el entorno digital, revelando cómo la recolección masiva de datos, el diseño adictivo de plataformas y la falta de regulación adecuada afectan su bienestar emocional, lo que exige un enfoque preventivo basado en derechos que garantice el consentimiento informado, reduzca brechas digitales y proteja la privacidad y salud mental de NNA frente a los riesgos del entorno digital.

El segundo capítulo explora de manera integral el impacto del entorno digital en la salud mental de niños, niñas y adolescentes en Ecuador, combinando análisis estadísticos, documental y entrevistas con expertos[6] para evidenciar cómo el crecimiento

[5] Ver Anexo 1.
[6] Ver Anexos 2, 3 y 4.

acelerado del acceso a Internet (especialmente impulsado por la pandemia) ha generado tanto oportunidades como desafíos. Se abordan cuestiones críticas como la sexualización temprana, la ansiedad, la depresión, el hiperconsumo y la violencia digital, resaltando las brechas territoriales y socioeconómicas que agravan estas problemáticas. Además, se enfatiza la importancia de una corresponsabilidad coordinada entre familias, Estado y empresas tecnológicas, y se plantean estrategias de cooperación internacional y políticas públicas que resultan esenciales para transformar este entorno digital en un espacio seguro y saludable para la población infantil y adolescente.

Por último, en el tercer capítulo se presenta la exigibilidad estratégica del derecho a la salud mental de niños, niñas y adolescentes en el entorno digital, planteándola como un proceso social, político y legal que, inspirado en la doctrina de los derechos humanos, articula cuatro grandes vías de actuación (jurídica [litigio estratégico, hábeas data y reclamos administrativos ante la Autoridad de Protección de Datos], social [campañas de sensibilización, talleres y movilizaciones continuas], política [activar instituciones de derechos humanos, fiscalización] e internacional [mecanismos de la ONU, Sistema Interamericano, convenios supranacionales]) para visibilizar violaciones estructurales, generar precedentes, empoderar a comunidades y ejercer presión normativa y regulatoria con el fin de garantizar una protección integral y sostenible de los datos personales de la niñez y adolescencia frente a los riesgos digitales.

# Capítulo primero
# Protección de datos personales y salud mental de niños, niñas y adolescentes en el entorno digital

Internet es la escena del crimen del siglo XXI
(Cyrus Vance Jr., 2014)

En este capítulo se articula cómo las grandes narrativas de cohesión social (desde las religiones hasta el liberalismo) cimentaron la dignidad y la libertad humanas, pero hoy se ven tensionadas por el *big data* y los algoritmos, que capturan y procesan masivamente datos personales para perfilar conductas y condicionar decisiones. Este modelo, denominado capitalismo de la vigilancia, convierte la información en el nuevo "petróleo", favoreciendo a corporaciones tecnológicas que, al monetizar predicciones de comportamiento, desplazan la voluntad individual y vulneran el principio kantiano de considerar a la persona como fin en sí misma. Frente a ello, el capítulo examina el derecho a la protección de datos personales en el ámbito internacional, nacional, y a través de un análisis comparado con el RGPD europeo, que resalta la gestión de riesgos y la responsabilidad proactiva. También se describen las obligaciones exclusivas del Estado (autoridades de control, cooperación transfronteriza) y las responsabilidades de empresas y delegados de datos para garantizar la legalidad, transparencia y derechos de los titulares.

A continuación, se aborda el derecho a la salud mental de niños, niñas y adolescentes en el entorno digital, ligándolo al uso y protección de sus datos personales. A nivel internacional, se recogen estándares de la Relatoría Especial de la ONU sobre salud, de los Comités DESC y del Niño, que exigen servicios accesibles y no coercitivos, así como evaluaciones de impacto digital que atenúen riesgos como la adicción, el ciberacoso o la explotación de metadatos. En el plano nacional, se analiza la Ley Orgánica de Salud Mental, su reglamento y políticas de protección infantil y adolescente en línea, constatando omisiones en la regulación de tecnologías digitales y en la participación efectiva de los NNA. Finalmente, se identifican desafíos pendientes: cerrar brechas digitales, fortalecer marcos legales que regulen contenidos nocivos y publicidad personalizada, garantizar el consentimiento informado de NNA y su autodeterminación informativa, e instaurar mecanismos preventivos y de rendición de cuentas que integren plenamente la dimensión psicosocial en las políticas públicas.

## 1. Aspectos conceptuales en torno a los derechos humanos, *big data* y algoritmos

Es innato del ser humano buscar el sentido de la vida, y a lo largo del tiempo ha construido diversas narrativas que han permitido generar cohesión social y, con ello, poder. Estas ficciones han sido fundamentales para facilitar la cooperación a gran escala, ya que permiten estructurar identidades colectivas que refuerzan la pertenencia y la acción conjunta. La organización social no se basa únicamente en hechos científicos o en necesidades económicas, sino en relatos compartidos que moldean la percepción del mundo y la forma en que las sociedades interactúan y evolucionan.[7]

De esta manera, se entiende por qué en tiempos premodernos las religiones contestaban las profundas preguntas ontológicas de la vida, para lo cual se debían leer las sagradas escrituras.[8] Actualmente, las religiones tradicionales han perdido terreno ante el relato liberal que considera a la libertad humana (de la cual emana intrínsecamente la dignidad), que queda consagrada en los derechos humanos y la democracia, como el valor más importante, pues sostiene que toda autoridad proviene en última instancia del libre albedrío, expresado en sentimientos, deseos y opciones.[9]

Ya no es necesario entonces leer las palabras de los dioses o de sus intérpretes, sino seguir la propia voluntad, vivir como se quiera, dignamente.[10] En otras palabras, en épocas anteriores el poder lo tenía Dios, sin embargo, debido a la gran influencia de los derechos humanos, tanto en su vertiente social como liberal, es innegable que el poder de decidir, al menos en teoría, ahora se le reconoce a cada ser humano, pues por el hecho de serlo tiene dignidad, que implica la libertad de decidir.

Por otro lado, el análisis y uso en general de la información generada y disponible en Internet plantea desafíos en torno a la protección de datos personales, en este punto toma relevancia el *big data* o macrodatos, término que se refiere a la masiva cantidad de datos generados en la red que son "susceptibles de ser capturados, almacenados, administrados, analizados y sistematizados en busca de tendencias y perfiles",[11]

---

[7] Yuval Noah Harari, "Religión", en *21 lecciones para el siglo XXI*, Debate (Colombia: Penguin Random House, 2008), 156.

[8] Ibíd., 157.

[9] Ibíd., 65.

[10] Ecuador Corte Constitucional del Ecuador, "T-881-02 Corte Constitucional de Colombia", *Corte Constitucional del Ecuador*, accedido 18 de noviembre de 2019, http://www.corteconstitucional.gov.co/relatoria/2002/t-881-02.htm.

[11] Relatoría Especial para la Libertad de Expresión CIDH, "Estándares para una Internet Libre, Abierta e Incluyente", 15 de marzo de 2017, 232-3, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiQyKKHgc_rA

demostrando así la gran velocidad y escala en la que operan los algoritmos que permiten predecir patrones de conducta (que pueden implicar control de voluntad y decisión).[12] Según estimaciones de la empresa IBM, diariamente se generarían alrededor de 2.5 mil millones de gigabytes de información,[13] y cada año se genera cada vez más información, entonces, el potencial del *Big data* es casi infinito, pues se puede aplicar a todas las áreas del conocimiento humano.

Desde la esfera económica, si se observa a las empresas con más patrimonio del mundo como *Apple*, *Amazon*, *Meta*, *Microsoft* o *Google*,[14] se puede notar que todas son empresas que lucran con datos, pues a medida que usuarios y usuarias utilizan sus servicios estas empresas recopilan su información, que luego analizan y procesan para desarrollar algoritmos, con los que pueden construir programas o aplicaciones según su interés.[15] Esto da como resultado que los datos sean el activo más importante en la presente época, convirtiéndose incluso en bienes más preciados que el petróleo,[16] el *Data Marketing*[17] es el nuevo mercado millonario. Esto demuestra que la acumulación de datos personales de millones de personas permite conocer a través de algoritmos sus patrones de conducta, convirtiéndose así en una forma de poder.

Un algoritmo se constituye en una serie de instrucciones definidas, ordenadas y finitas para solucionar algún problema, realizar un cálculo, procesar datos y llevar a cabo otras tareas o actividades,[18] pero los humanos también se guían por algoritmos. El siglo

---

hWGwVkKHfr2BxAQFjAAegQIBxAB&url=http%3A%2F%2Fwww.oas.org%2Fes%2Fcidh%2Fexpresion%2Fdocs%2Fpublicaciones%2FInternet_2016_esp.pdf&usg=AOvVaw3NnuAYlvGay9-fr_a8dyMC.

[12] Diego Nicolás Castillo Warnken, "Caracterización y predicción de conducta de usuarios de aplicación móvil enfocado a proceso "on boarding" utilizando herramientas de Machine Learning", 2022.

[13] Discovery en Español, "¿Sabes qué es Big Data?", *Discovery*, accedido 4 de septiembre de 2020, https://www.youtube.com/watch?v=Ju2oDsHAL-o.

[14] *FXSSI*, "Las empresas más valiosas del mundo - 2019", *FXSSI - Indicador de Sentimiento de Forex*, accedido 19 de noviembre de 2019, párr. 1, https://es.fxssi.com/las-empresas-mas-valiosas-del-mundo.

[15] Daniel Cana, "¿Por qué los datos de las personas normales valen más que el petroleo?", *Thingeer*, 9 de agosto de 2019, párrs. 1-3, https://blog.thingeer.com/por-que-los-datos-de-las-personas-normales-valen-mas-que-el-petroleo/.

[16] Netflix, "Nada es privado: Documental", *Netflix*, 2019, https://www.netflix.com/watch/80117542?trackId=13752289&tctx=0%2C0%2C6eba89d7-924d-46fb-b19a-ea1cc2e03a55-16740837%2C%2C.

[17] El concepto hace referencia a "las técnicas, procesos, herramientas y tecnología de procesamiento de la información en grandes volúmenes de datos en tiempo real que nos permiten analizar aspectos tan importantes para una marca como el comportamiento de los consumidores y, de este modo, poder llevar a cabo estrategias que les permitan atraerlos e incrementar sus ventas", aunque se puede utilizar para diversos fines, como para campañas políticas. En "¿Qué es el Big Data Marketing y qué ventajas ofrece?", *SEMrush Blog*, accedido 19 de noviembre de 2019, párr. 8, https://es.semrush.com/blog/que-es-big-data-marketing-ventajas/.

[18] David J. Malan, "Tu cerebro puede hacer algoritmos", *Video de YouTube*, 2013, https://www.youtube.com/watch?v=6hfOvs8pY1k.; BBC Learning, "What Is An Algorithm", 2015,

XXI está dominado por los algoritmos. Incluso las emociones son algoritmos bioquímicos que se han desarrollado a lo largo de los años para la supervivencia y reproducción, en este sentido, un algoritmo es "un conjunto metódico de pasos que pueden emplearse para hacer cálculos, resolver problemas y alcanzar decisiones […] No es un cálculo concreto, sino el método que se sigue cuando se hace el cálculo".[19] Otros autores afirman que un algoritmo es una opinión incrustada en matemáticas.[20] Para construir un algoritmo se necesita información y una definición de éxito, que dependerá del creador del algoritmo. Quienes construyen los algoritmos generalmente provienen de un grupo homogéneo de un entorno corporativo que tienen interés de lucro, más allá de generar beneficio para las personas consumidoras de sus servicios; por este motivo considera que se debe cuestionar los propios algoritmos e incluir a la ética en la construcción de estos, especialmente cuando somos guiados a diario por los mismos.[21]

Así, el problema radica en la monopolización de estas inmensas bases de datos, que, al ser capaces de predecir comportamientos mediante algoritmos, también pueden influenciar el comportamiento de las personas que consumen sus servicios de acuerdo con sus intereses,[22] y no en función del ser humano, tomando a este como medio y no como un fin en sí mismo, por lo que es contrario a la máxima kantiana, que tiene una directa relación con los derechos humanos.

### 1.1 Capitalismo en la digitalización de la sociedad

El fenómeno de la digitalización ha generado un modelo económico denominado capitalismo de la vigilancia, en el que las experiencias personales se convierten en datos comercializables. A través de algoritmos, estos datos permiten predecir comportamientos futuros, que son vendidos a empresas con fines lucrativos.[23] Este sistema se basa en la

---

https://www.youtube.com/watch?v=Da5TOXCwLSg.; Suayed, "Análisis, diseño e implementación de algoritmos", 2017.; Unam Coordinación de Universidad Abierta y Educación a Distancia, "Problemas y Algoritmos", s.f., https://programas.cuaed.unam.mx/repositorio/moodle/pluginfile.php/1163/mod_resource/content/1/contenido/index.html; Khan Academy, "Algoritmos: Ciencias de la computación", *Khan Academy*, accedido 6 de junio de 2023, https://es.khanacademy.org/computing/computer-science/algorithms.

[19] Yuval Noah Harari, "El Antropoceno", en *Homo Deus. Breve historia del mañana*, Debate (Colombia: Penguin Random House, 2018), 100.

[20] Cathy O'Neil, "The Truth About Algorithms", *Video de YouTube*, 2018, https://www.youtube.com/watch?v=heQzqX35c9A.

[21] Ibíd.

[22] Carlos Saura García, "El lado oscuro de las GAFAM: monopolización de los datos y pérdida de privacidad", *Veritas*, n.º 52 (2022): 17, doi:10.4067/S0718-92732022000200009.

[23] Shoshana Zuboff, fundadora del concepto, es profesora emérita de la *Harvard Business School.* Su libro *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*

vigilancia constante de la vida privada, apropiándose de información personal bajo prácticas que han sido cuestionadas por su legitimidad. [24]

Este derivado del capitalismo, que amenaza a la libertad de las personas porque condiciona su conducta, fue originado hace aproximadamente 20 años, durante la crisis de las puntocom,[25] cuando *Google* se encontraba en busca de un método rentable para otorgar sus servicios en la red sin que impliquen un costo a sus usuarios,[26] por lo que vendió sus predicciones con la información que poseía de sus usuarios en un primer momento a empresas de publicidad personalizada. Esta fórmula lucrativa redimensionó el negocio del Internet y por primera vez se pudo predecir y modificar el comportamiento del consumidor utilizando un algoritmo, naciendo así la analítica predictiva. Ahora, este tipo de capitalismo se encuentra presente en cada producto *Smart* y en cada servicio personalizado,[27] por lo que se extiende más allá del Internet.[28]

> El capitalismo de la vigilancia se convirtió en el modelo dominante. Primero Google, después Facebook, posteriormente todo el sector tecnológico. Con los beneficios de la vigilancia los inversores generan más ganancias, y lo hacen más rápido que con el capitalismo clásico, en el que se comercializan productos y servicios que la gente realmente necesita.[29]

La falta de regulación sobre las grandes corporaciones tecnológicas ha permitido que sus decisiones se rijan principalmente por el interés económico, sin considerar los impactos negativos que pueden generar. En Silicon Valley, existe la creencia de que las buenas intenciones de los desarrolladores y ejecutivos son suficientes para garantizar resultados positivos; [30] sin embargo, la realidad ha demostrado lo contrario. La influencia de las redes sociales en procesos electorales y la propagación de desinformación han

---

fue publicado en enero de 2019. En Lucía Blasco, "Qué es el 'oscuro' capitalismo de la vigilancia de Facebook y Google y por qué lo comparan con la conquista española", *BBC News Mundo*, 1 de marzo de 2019, párr. 32, https://www.bbc.com/mundo/noticias-47372336.

[24] DW Documental, "Google, Facebook, Amazon - El poder ilimitado de los consorcios digitales", *Vídeo de YouTube*, 2022, https://www.youtube.com/watch?v=A3cGMNxRNJ0.

[25] Así se le llamó al incremento rápido que tuvieron las empresas de Internet de 1998 a 2001, produciendo una burbuja especulativa que termino reventando. Blasco, "Qué es el 'oscuro' capitalismo de la vigilancia de Facebook y Google y por qué lo comparan con la conquista española", párr. 9.

[26] VPRO Documental, "Shoshana Zuboff sobre el capitalismo de vigilancia", 2019, *Vídeo de YouTube*, https://www.youtube.com/watch?v=hIXhnWUmMvw&feature=youtu.be.

[27] Blasco, "Qué es el 'oscuro' capitalismo de la vigilancia de Facebook y Google y por qué lo comparan con la conquista española", párr. 25.

[28] Es preciso aclarar que la tecnología digital no equivale al capitalismo de la vigilancia, pues el problema radica en el uso que se le da, y no en la tecnología como tal.

[29] DW Documental, "Google, Facebook, Amazon - El poder ilimitado de los consorcios digitales".

[30] Ibíd.

tenido efectos graves en la sociedad, como se evidenció durante la pandemia. Cuando el objetivo principal es la rentabilidad, la manera en que se difunde la información responde únicamente a criterios comerciales, dejando de lado las consecuencias sociales y políticas, lo que puede resultar en daños irreparables. Como acto de protesta, se han llevado a cabo intervenciones públicas, como la colocación de bolsas para cadáveres frente a las oficinas de Facebook en Washington, para visibilizar los peligros que conlleva esta falta de control. [31]

Otros autores han desarrollado el concepto "economía de la atención", para describir los problemas de la sociedad de la información, en donde se construye un oligopolio sobre los bienes de la información, es decir, los datos. [32] Desde esta perspectiva, la atención es otro mercado, de la cual las redes sociales "generan más beneficios cuanto más tiempo logran enganchar a los usuarios",[33] por eso emplean diseños y estrategias en sus interfaces que logran captar y controlar la atención;[34] esto puede producir afectaciones en la atención que pueden afectar a la salud, además de generar un oligopolio de la atención a ciertas redes sociales como *Facebook, Instagram* o *Tik Tok.*

El concepto del panóptico, originalmente propuesto por Bentham,[35] ha sido retomado para describir el feudalismo digital actual, en el que la sociedad se encuentra sometida a una vigilancia global constante. A diferencia del modelo clásico, donde la observación es unilateral y disciplinaria, en el entorno digital, la vigilancia se vuelve omnipresente y personalizada, con plataformas que no solo registran el comportamiento de los usuarios, sino que también anticipan sus deseos y pensamientos.[36] En este contexto, las redes sociales desempeñan un papel central, funcionando como herramientas que

---

[31] Ibíd.

[32] Cristina Fernández-Rovira, "Motivaciones y tiempo de uso de las redes sociales por parte de los niños, niñas y adolescentes españoles: señales de adicción", *Anuario Electrónico de Estudios en Comunicación Social 'Disertaciones'"* 15, n.º 2 (11 de julio de 2022), doi:10.12804/revistas.urosario.edu.co/disertaciones/a.11155, 6, citado en Santiago Giraldo-Luque y Cristina Fernández-Rovira, "Redes sociales y consumo digital en niños, niñas y adolescentes universitarios: Economía de la atención y oligopolios de la comunicación en el siglo XXI", *Profesional de la información* 29, n.º 5 (3 de noviembre de 2020), doi:10.3145/epi.2020.sep.28.

[33] Ibíd., 5.

[34] Como las notificaciones, que abarcan la atención e induce a un estado de sobre alerta que puede desembocar en ansiedad; ibíd., 5.

[35] Panóptico, del latín pan=todo y óptico=visión, es un modelo de cárcel (que jamás llegó a construirse) creado por Bentham (padre de la vigilancia social moderna), en la que todo se puede vigilar desde un único punto, sin ser visto ni oído, lo que hace que la conducta de los vigilados se modifique. José Alcántara, "El panóptico, la cárcel perfecta de Jeremy Bentham", *Versvs*, 11 de abril de 2007, párr. 3, https://www.versvs.net/panoptico-carcel-perfecta-jeremy-bentham/.

[36] Byung-Chul Han, "Psicopolítica: Neoliberalismo y nuevas técnicas de poder", *Ebsco*, 2014, 50, https://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=1544689.

facilitan la recolección masiva de datos y la modelación del comportamiento individual y colectivo.[37]

Además, considera que la pandemia aceleró la aplicación del régimen de vigilancia biopolítica, es decir, de un sistema que busca acceder de manera ilimitada al individuo, ya que no solo las comunicaciones están siendo vigiladas digitalmente, sino también los cuerpos, sobre todo en países asiáticos como China.[38] Por eso se considera que "el *Big Data* anuncia el fin de la persona y de la voluntad libre",[39] pues a partir de los macrodatos se exhiben los patrones de comportamiento colectivos de los que el individuo no es consciente, por lo que se podría explotar su psique[40] y así manipular los comportamientos de estos.

Todos estos conceptos han sido considerados en el presente estudio porque sirven para explicar por qué es un problema para los derechos humanos que las nuevas tecnologías sean utilizadas por las empresas de datos para sustraer y mercantilizar datos personales de sus usuarios sin su conocimiento ni consentimiento, lo que implica una grave vulneración del derecho a la protección de datos personales, que a su vez puede llegar a vulnerar otros derechos según cómo se utilice esta información, por lo que se considera esencial analizar el contenido y alcance de este derecho ante estas circunstancias. Además, esta situación se agrava si se observa que existe una tendencia a concentrar las inmensas bases de datos.[41]

---

[37] Clarín, "Byung-Chul Han: Vamos hacia un feudalismo digital y el modelo chino podría imponerse", *Clarín*, 14 de abril de 2020, párr. 9, https://www.clarin.com/cultura/byung-chul-vamos-feudalismo-digital-modelo-chino-podria-imponerse_0_QqOkCraxD.html?fbclid=IwAR0dXGUP0PLeyHLfDZed_aLWp9eaD5BpUpHbpVcY5RqAg1eFJgW0fx5TtNI.

[38] Ibíd., párr. 13.

[39] Byung-Chul Han, "Psicopolítica", 14.

[40] Ibíd., 51.

[41] Ver Diego Alonso García Ramírez y Santiago Giraldo Luque, "Presentación del número: la economía de la atención en un Internet monopolizado", *Anuario Electrónico de Estudios en Comunicación Social*: *Disertaciones* 15, n.º 2 (2022), doi:10.12804/revistas.urosario.edu.co/disertaciones/a.11964.

## 2. Contenido y alcance del derecho a la protección de datos personales

Nos encontramos ante el fin de una era y el inicio de otra, debido a la confluencia de dos revoluciones, el de la biotecnología[42] y de la infotecnología,[43] que con la información adecuada tienen la capacidad plena (poder) de producir algoritmos que pueden supervisar y comprender sentimientos mejor que un ser humano, lo que puede conllevar a que la autoridad pase de los humanos a los ordenadores, desintegrando la noción de libertad.[44] Se pueden observar, en este punto, claros ejemplos de lo manifestado, pues ya en algunas circunstancias de nuestra vida algoritmos deciden por nosotros.[45]

Frente a este cambio de época, ante el cual el relato de los derechos humanos no se encuentra en circunstancias deseables para seguirse desarrollando, es imprescindible considerar el contenido y alcance del derecho a la protección de datos personales. Éste es un derecho humano que se deriva del derecho (humano) a la privacidad, reconocido en varios instrumentos internacionales de derechos humanos, como en el artículo 12 de la Declaración Universal de Derechos Humanos,[46] en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos -PIDCP-,[47] en el artículo 8 de la Convención Europea de

---

[42] La Convención sobre Diversidad Biológica de 1992 en su segundo artículo define a la biotecnología como "toda aplicación tecnológica que utilice sistemas biológicos y organismos vivos o sus derivados para la creación o modificación de productos o procesos para usos específicos". En "Convenio sobre Diversidad Biológica", 2 de noviembre de 2006, https://www.cbd.int/convention/articles/?a=cbd-02.. Es un área multidisciplinaria que emplea biología, química y procesos varios con uso en agricultura, farmacia, alimentos, ciencias forestales y medicina. En "¿Qué Es La Biotecnología?", *Centro de Biotecnología*, 12 de noviembre de 2019, párr. 1, https://www.centrobiotecnologia.cl/comunidad/que-es-la-biotecnologia/.

[43] Según la *Information Technology Association of America* (ITAA), la Infotecnología es "el estudio, diseño, desarrollo, implementación, soporte o dirección de los sistemas de información computarizados, en particular de software de aplicación y hardware de computadoras". Es un término general que describe cualquier tecnología que ayuda a producir, manipular, almacenar, comunicar o esparcir información, cuya utilización se ha extendido a todos los ámbitos de la sociedad y forma parte de la cultura de las actuales generaciones. En "Concepto de Infotecnología", *Infotecnología La Revolución Tecnológica*, 19 de marzo de 2016, párr. 1, https://tecnologiaeducativawordpreescom.wordpress.com/2016/03/19/concepto-de-infotecnologia/.

[44] Harari, *21 lecciones para el siglo XXI*, 70.

[45] Por ejemplo, a la hora de ver YouTube o Netflix, sus algoritmos nos recomiendan qué ver en base a lo que hemos visto, o dado me gusta, además de relacionarnos con nuevo contenido que podría gustarnos según la información que otorgamos. Google Maps o Waze nos marcan el camino para llegar al lugar deseado, o *Tinder* nos indica perfiles de personas que según su algoritmo pueden ser compatibles.

[46] ONU Asamblea General, "Declaración Universal de Derechos Humanos", 10 de diciembre de 1948, Resolución 217 (A) III, art. 12.

[47] ONU Asamblea General, "Pacto Internacional de Derechos Civiles y Políticos", 16 de diciembre de 1966, Resolución 2200A (XXI), art. 17.

Derechos Humanos,[48] en el artículo 11 de la Convención Americana sobre Derechos Humanos,[49] entre otros.[50]

Esta sección aborda los principales instrumentos que regulan el derecho a la protección de datos personales, así como los estándares y principios interpretativos que orientan las obligaciones de los Estados y las empresas.

### 2.1. Marco de Protección Internacional de Protección de Datos Personales

A nivel internacional se encuentran diversos instrumentos que se han referido al derecho a la privacidad. Con respecto al Sistema Universal de Derechos Humanos (SUDH), la Asamblea General de Naciones Unidas se ha referido a la inteligencia artificial, e insta a todos los Estados Miembros a fomentar "el desarrollo, la aplicación y la divulgación de mecanismos de seguimiento y gestión de los riesgos, mecanismos para la protección de los datos, incluida la protección de los datos personales y políticas de privacidad, y evaluaciones de impacto según proceda",[51] de modo que se proteja la privacidad y se garantice la protección de los datos personales al poner a prueba y evaluar estos sistemas.[52]

También es importante considerar las resoluciones del Consejo de Derechos Humanos (A/HRC/32/L.20) y de la Asamblea General (A/RES/68/167), que establecen que todos los derechos humanos deben ser protegidos en el entorno digital. El informe del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, denominado "El derecho a la privacidad en la era digital", presentado en 2018 al Consejo de Derechos Humanos (A/HRC/39/29), resalta la importancia de la transparencia y la rendición de cuentas en la vigilancia de las comunicaciones.

Asimismo, la Observación N°16 del CDH define conceptos clave del derecho a la privacidad en el marco del Pacto Internacional de Derechos Civiles y Políticos y subraya la necesidad de que la recopilación de datos esté reglamentada por la ley, permitiendo a

---

[48] Tribunal Europeo de Derechos Humanos, "Convenio Europeo de Derechos Humanos", 1950, art. 8.

[49] Organización de los Estados Americanos, "Convención Americana sobre Derechos Humanos", 22 de noviembre de 1969, art. 11.

[50] Asimismo, existen instrumentos normativos que reconocen este derecho a sujetos específicos, como el artículo 16 de la Convención sobre los Derechos del Niño -CRC- y el artículo 22 de la Convención sobre los Derechos de las Personas con Discapacidad -CRPD-.

[51] ONU Asamblea General, "Aprovechar las oportunidades de sistemas seguros, protegidos y fiables de inteligencia artificial para el desarrollo sostenible", 11 de marzo de 2024, A/78/L.49, párr. 6. e.

[52] Ibíd., párr. 6. j.

los individuos verificar y solicitar la rectificación o eliminación de su información. Por su parte, el Informe del Relator sobre el derecho a la privacidad, presentado al Consejo de Derechos Humanos en 2019 (A/HRC/40/63), especifica principios fundamentales como la legalidad, necesidad, proporcionalidad y limitación de la finalidad en el tratamiento de datos.

En lo que respecta al sistema interamericano, es fundamental considerar el Informe Anual de la Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de 2013 (OEA /Ser.L/V/II.149), que en su cuarto capítulo aborda la relación entre la privacidad, la protección de datos personales y la libertad de expresión en Internet, estableciendo límites a la vigilancia masiva y resaltando la necesidad de salvaguardar la privacidad como condición para el ejercicio pleno de otros derechos fundamentales.

Uno de los instrumentos que otorgan mayor protección al derecho a la protección de datos personales es el de Principios Actualizados del Comité Jurídico Interamericano sobre la Privacidad y la Protección de Datos Personales del Comité Jurídico Interamericano, de abril de 2021.[53] Estos principios reflejan las distintas perspectivas adoptadas por los Estados miembros en relación con aspectos clave de la protección de datos personales, como el consentimiento, los fines y métodos de recolección y procesamiento, la transferencia internacional de datos, su seguridad, la salvaguarda de información sensible y el ejercicio de derechos como el acceso, rectificación, cancelación, oposición y portabilidad.

Especial importancia tiene el principio dos de este instrumento, que se refiere a la transparencia y el consentimiento respecto de la recopilación de datos personales. Este estándar tiene una importancia especial teniendo en cuenta que el informe de investigación tiene como sujetos de derechos a los niños, niñas y adolescentes, personas que a nivel nacional son considerados como incapaces absolutos o relativos,[54] por lo que se establecen protecciones especiales para estas personas con el fin de obtener su consentimiento, indicando que se debe obtener la autorización del titular de la patria potestad, que él o la titular puede revocar su consentimiento en cualquier momento y que

[53] Comité Jurídico Interamericano OEA, "Principios Actualizados del Comité Jurídico Interamericano sobre la Privacidad y la Protección de Datos Personales, con Anotaciones", Pub. L. No. CJI/DOC.638/21 (2021).

[54] Ecuador, *Código Civil*, Registro Oficial 46, Suplemento, 24 de junio de 2005, art. 1463.

el método para obtener el consentimiento debe ser apropiado para la edad y capacidad de la persona afectada.[55]

En la misma línea, el Sistema Interamericano de Derechos Humanos (SIDH) a través de la Corte Interamericana de Derechos Humanos (CorteIDH), basándose en los Principios Actualizados del Comité Jurídico Interamericano sobre Privacidad y la Protección de Datos Personales, ha establecido en el Caso Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo Vs. Colombia" que:

> Los estándares internacionales en materia de protección de datos personales exigen que su recopilación, almacenamiento, tratamiento y divulgación sea factible solamente ante el consentimiento libre e informado del titular de los datos o, en su defecto, derivado de un marco normativo que faculte expresamente a los organismos públicos para desarrollar tales acciones. En todo caso, la obtención y gestión de datos personales solo se autoriza, en el marco de la Convención Americana, para la consecución de fines legítimos y por mecanismos legales[56]

Esta sentencia de la CorteIDH es importante debido a que reconoce a la autodeterminación informativa como un derecho autónomo, pese a que no se encuentra establecido expresamente en la Convención Americana sobre Derechos Humanos (CADH). La CorteIDH indicó que el derecho a la autodeterminación informativa está respaldado por la Convención Americana, especialmente a través de los derechos a la protección de la honra y al acceso a la información, establecidos en los artículos 11 y 13 respectivamente, así como en el derecho a la protección jurisdiccional conforme al artículo 25. Este derecho es independiente y a su vez garantiza otros derechos, como la privacidad, la honra, la reputación y, en general, la dignidad de la persona. La autodeterminación informativa incluye el derecho a acceder y controlar los datos personales en posesión de entidades públicas, así como también opera en relación con registros o bases de datos mantenidos por entidades privadas.[57]

También existen instrumentos fuera del sistema interamericano y universal; por ejemplo, los Estándares de Protección de Datos Personales para los Estados Iberoamericanos, de junio de 2017[58] de la Red Iberoamericana de Protección de Datos

---

[55] Comité Jurídico Interamericano OEA, "Principios Actualizados del Comité Jurídico Interamericano sobre la Privacidad y la Protección de Datos Personales, con Anotaciones", 33.

[56] Corte Interamericana de Derechos Humanos, *Caso Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" Vs. Colombia*, 18 de octubre de 2023, párr. 573.

[57] Ibíd., párrs. 586-7.

[58] Red Iberoamericana de Protección de Datos, "Estándares de Protección de Datos Personales para los Estados Iberoamericanos", 2017.

(RIPD) (de la cual Ecuador es parte).[59] Si bien este documento no se configuran como convenio, el artículo 426 de la Constitución establece que se deben aplicar los instrumentos internacionales de derechos humanos que señalen una mejor protección a la establecida en la Constitución,[60] lo que implica que este documento un indudable valor jurídico.

El Convenio 108+, que es la versión modernizada del Convenio 108, adoptado por el Consejo de Europa en 1981,[61] tiene como objetivo proteger la privacidad de los individuos y garantizar el respeto de sus derechos humanos en relación con el tratamiento de sus datos personales.[62] La versión actualizada, 108+, refuerza estas protecciones y se adapta a los desafíos y tecnologías modernas.

No obstante, no cabe duda de que el Reglamento General de Protección de Datos de la Unión Europea (RGPD) de la UE es el instrumento normativo más avanzado, pues recoge todos los estándares anteriormente mencionados. Este documento, que "responde a una larga evolución sobre la protección de datos personales en la Unión Europea de más de 40 años",[63] entró en vigencia el 25 de mayo de 2018. Este instrumento reemplaza la Directiva 95/46/CE sobre protección de datos de 1995 de la Unión Europea, con el propósito de reforzar la protección del derecho a la protección de datos personales e impulsar la economía digital en la UE.[64]

El RGPD, que recoge instituciones como la aplicación extraterritorial,[65] el derecho al olvido,[66] responsabilidad de la empresa,[67] la portabilidad de datos[68] y el consentimiento

---

[59] Red Iberoamericana de Protección de datos, "Países miembros", *REDIPD*, accedido 30 de noviembre de 2024, https://www.redipd.org/es/enlaces-de-interes/paises-miembros.

[60] Ecuador, *Constitución de la República del Ecuador*, art. 426.

[61] Consejo Europeo, "Details of Treaty No.108", *Treaty Office*, accedido 7 de octubre de 2024, párr. 5, https://www.coe.int/en/web/conventions/full-list.

[62] Consejo Europeo, "Convention for the protection of individuals with regard to the processing of personal data", junio de 2018, art. 1.

[63] Luis Enríquez Álvarez, "La Visión de América Latina sobre el Reglamento General de Protección de Datos", *Comentario Internacional* n.° 19 (2019): 99-112, doi:10.32719/26312549.2019.19.4, 100.

[64] Ibíd., 101.

[65] El RGPD se aplica a todas las empres que procesan los datos personales de ciudadanos de la Unión Europea, incluso si la empresa no está ubicada en la Unión Europea. En Parlamento Europeo y Consejo Europeo, "Reglamento General de Protección de Datos", L 119/1 § (2016), art. 3.

[66] Derecho a solicitar la eliminación de datos personales, siempre que no exista razón legal para mantenerlos. Ibíd., art. 17.

[67] Las empresas deben tomar medidas para proteger los datos personales de los ciudadanos, y en caso de una brecha de seguridad, deben notificar a las autoridades competentes y a los ciudadanos afectados; ibíd., art. 24.

[68] Derecho a recibir una copia de los datos personales en un formato que permita transferirlos a otra empresa; ibíd., art. 20.

informado,[69] establece un marco legal sólido para la protección de datos personales, al otorgar a los ciudadanos de la Unión Europea (UE) una serie de derechos en relación con sus datos personales, como el derecho a acceder a sus datos, de rectificarlos, borrarlos u objetar su procesamiento. Además, impone a las empresas y organizaciones que recopilan datos sanciones en caso de que no cumplan con el reglamento. Asimismo, su alcance extraterritorial permite que instituciones públicas y privadas de todo el mundo deban cumplir con las obligaciones en él establecidas, incluidas las latinoamericanas. La Ley Orgánica de Protección de Datos Personales (LOPDP) incorporó mucho de su contenido y lo adaptó a la realidad nacional.

Por último, es importante mencionar normativas de otros países, que, aunque no son vinculantes para el Ecuador, poseen avances significativos en esta materia. En Estados Unidos existe la Ley de Privacidad del Consumidor de California (CCPA), que es especialmente importante toda vez que regula a las empresas de Silicon Valley como *Meta*. Este cuerpo legal establece derechos de privacidad para los consumidores de este Estado y obliga a las empresas que procesan los datos personales de estos consumidores a cumplir con ciertas reglas de protección de datos.

### 2.2. Marco de Protección Nacional de Protección de Datos Personales

La Constitución ecuatoriana no reconoce expresamente en ninguno de sus artículos el derecho a la privacidad, aunque sí reconoce el derecho a la intimidad personal[70] y a la protección de datos personales.[71] Esto sucede debido a que el país ha desarrollado un modelo mixto entre el modelo anglosajón, en el que se debe demostrar la afectación a la vida privada para que el Estado tome acción, y el sistema europeo, que a diferencia del anglosajón, ha desarrollado un derecho diferente al de privacidad, pero que se deriva de este, para proteger los datos personales en la web.

Este derecho, desarrollado en el sistema europeo, se denomina autodeterminación informativa, y se centra en la libre voluntad del titular de derechos de decidir sobre su información personal, sin necesidad de justificar una vulneración de derechos.[72] Se

---

[69] Las empresas deben obtener el consentimiento explícito e informado de los ciudadanos antes de recopilar y procesar sus datos personales; ibíd., art. 7.

[70] Ecuador, *Constitución de la República del Ecuador*, Registro Oficial 449, 20 de octubre de 2008, art. 69, num. 20.

[71] Ibíd., art. 66, num. 19.

[72] Lorena Naranjo, "Ponencia: Proyecto de ley de protección de datos personales", accedido 23 de septiembre de 2020, https://www.facebook.com/salim.zaidan/videos/10157069142610896/. Lorena

comprende entonces que cada persona tiene la libertad de participar en el proceso de recolección de datos y asegurar su veracidad, que se utilice para fines lícitos y que no sean empleados de forma que invada el espacio de privacidad que toda persona debe tener garantizado.[73] Este derecho de carácter preventivo es el que se encuentra reconocido en la Constitución al afirmar que la protección de datos personales incluye el acceso y la decisión sobre datos de este carácter, así como la autorización del titular o de la ley para la recolección, archivo, procesamiento, distribución o difusión de estos datos.[74]

En este sentido, el 10 de mayo de 2021 el pleno de la Asamblea Nacional aprobó, con 118 votos a favor, la Ley Orgánica de Protección de Datos Personales, impulsada por la Dirección Nacional de Registros Públicos. Esta norma entró en vigencia el 26 de mayo de 2021 y está compuesta por 12 capítulos y 77 artículos. Tiene sus antecedentes en el Plan Nacional de la Sociedad de la Información y el Conocimiento 2018-2021, cuyo eje estratégico N°6 tenía el propósito de generar una Ley Orgánica de Protección de Datos Personales.[75] Esta ley ordena la creación de institucionalidad,[76] como la Superintendencia de Protección de Datos, encargada de desarrollar políticas públicas para garantizar el derecho a la protección de datos personales, reconocido en el numeral 19 del artículo 66 de la Constitución.[77]

Así, el presidente Noboa mediante Oficio No T. 004-SGJ-24-0072 remitió la terna al Consejo de Participación Ciudadana y Control Social (CPCCS) el 29 de enero de 2024,[78] conforme al artículo 77 de la LOPDP, para que esta entidad elija al primer Superintendente de Protección de Datos. Así, el 28 de marzo de 2024 el pleno del CPCCS,

---

Naranjo Godoy, "El dato personal como presupuesto del derecho a la protección de datos personales y del hábeas data en Ecuador", Foro. Revista de Derecho 27 (2017), 70.

[73] Rosa Elena De la Torre y Juan Montaña Pinto, "El habeas data en Ecuador", en *Apuntes de derecho procesal constitucional*, t. 2 (Quito: CEDEC, 2012), 183-4.

[74] Ecuador, *Constitución de la República del Ecuador*, art. 66, num. 19.

[75] Mario Ramiro Aguilar Martínez et al., "La protección de datos personales en Ecuador", *Estudios del Desarrollo Social: Cuba y América Latina* 10, número especial 1 (2022), https://revistas.uh.cu/revflacso/article/view/3594, 375-6.

[76] La LOPDP establece un sistema de protección de datos personales, una Superintendencia de Protección de Datos y un Registro Nacional de Protección de Datos Personales (RNPDP). En Ecuador, *Ley Orgánica de Protección de Datos Personales*, Registro Oficial 459, Suplemento, 26 de mayo de 2021, arts. 5-51-77.

[77] El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley. En Ecuador, *Constitución de la República del Ecuador*, art. 66, num. 19.

[78] Consejo de Participación Ciudadana y Control Social, "Proceso de Selección del Superintendente de Protección de Datos", *CPCCS*, accedido 1 de marzo de 2024, https://www.cpccs.gob.ec/designacion-de-autoridades/super-proteccion-datos/.

por unanimidad, designó al Dr. Fabrizio Peralta Díaz como el primer titular de la Superintendencia de Protección de Datos Personales.[79] Esta normativa, incluido su régimen sancionatorio, debió haberse aplicado desde el 21 de mayo de 2023, es decir, dos años después de la entrada en vigencia de la LOPDP.[80] Sin embargo, debido a falta de financiamiento,[81] la Superintendencia de Protección de Datos Personales se consolidó en octubre de 2024.[82]

A nivel nacional también se han promulgado otros instrumentos, como la Política de Ciberseguridad por parte del Ministerio de Telecomunicaciones en mayo de 2021, que tiene el objetivo de "construir y fortalecer las capacidades nacionales que permitan garantizar el ejercicio de los derechos y libertades de la población y la protección de los bines jurídicos del Estado en el ciberespacio".[83] El mismo documento establece que la Subsecretaría de Gobierno Electrónico y Registro Civil debe implementar la Política de Ciberseguridad,[84] asentada en 7 pilares, en su mayoría desde una perspectiva de seguridad

---

[79] Fabrizio Peralta Díaz "es doctor en Derecho; máster en Estudios Estratégicos y Seguridad Internacional; ha cursado programas de posgrado en Liderazgo para la Transformación, Gobernanza, Liderazgo Político y Derecho Digital. Fue asesor de la Secretaría Jurídica de la Presidencia de la República; y de la Cámara de Comercio de Guayaquil; director jurídico de la Cámara de Industrias de Guayaquil; es árbitro en el Centro de Arbitraje y Mediación de la Cámara de Comercio de Quito. Es catedrático universitario". Nótese que no tiene experiencia en derechos humanos. En Consejo de Participación Ciudadana y Control Social, "Fabrizio Peralta Díaz es el primer superintendente de Protección de Datos", accedido 1 de mayo de 2024, https://www.cpccs.gob.ec/2024/03/fabrizio-peralta-superintendente/.

[80] Ecuador, *Ley Orgánica de Protección de Datos Personales*, Registro Oficial 459, Suplemento, 26 de mayo de 2021, Disposición Transitoria Primera.

[81] El Superintendente ha hecho un llamado urgente a las autoridades competentes para que se asignen los recursos financieros y materiales necesarios para el funcionamiento de la Superintendencia de Protección de Datos. Al respecto la Primera Autoridad de Protección de Datos (Superintendente), en su discurso de posesión en la Asamblea Nacional el 23 de abril de 2024, solicitó que se prevea el financiamiento a la Superintendencia de Protección de Datos de la siguiente manera: "(…) La Autoridad de Protección de Datos Personales, que de momento solo existe en el papel, tiene un amplio espectro de actuación. Son muchas sus atribuciones y variados sus deberes. No podrá pues, llevar a cabo su accionar, sin los recursos indispensables para su arranque y ulterior mantenimiento. Ello, desde luego adaptándose a la época de austeridad que la nación demanda. Sin embargo, no puedo dejar pasar esta oportunidad excepcional para exhortar a los funcionarios competentes a que provean los medios financieros y materiales que permitan cumplir la tarea que nos impone la Constitución y la Ley". Asimismo, en entrevistas Peralta Díaz ha manifestado que la Superintendencia de Protección de Datos Personales necesita una suma de al menos 2 millones de dólares, que implicaría la contratación de 30 a 35 personas. En Fabrizio Peralta-Díaz, "Post de LinkedIn", *Linkedin*, accedido 12 de junio de 2024, https://acortar.link/kSMh7O; en VASM, "Superintendente sin Superintendencia", 2024, *video de YouTube*, https://www.youtube.com/watch?v=f7Bk4Jf-3QE.

[82] Superintendencia de Protección de Datos Personales, "Superintendencia de Protección de Datos Personales", *Post de LinkedIn*, accedido 19 de octubre de 2024, https://acortar.link/mRigQI

[83] Ecuador Ministerio de Telecomunicaciones y de la Sociedad de la Información, "Política de Ciberseguridad", Acuerdo Ministerial 006-2021 § (2021), https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Acuerdo-No.-006-2021-Politica-de-Ciberseguridad.pdf, art. 2.

[84] Ibíd., art. 3.

y empresarial, más no de derechos humanos.[85] En el mismo sentido, el 3 de febrero de 2023 entró en vigencia la Ley Orgánica para la Transformación Digital y Audiovisual (LOTDA), cuya rectoría la ejerce el Ministerio de Telecomunicaciones,[86] y al igual que la Política de Ciberseguridad, posee un enfoque empresarial, donde se busca promover la inversión.[87]

El Ecuador ha dado un paso significativo en la protección de datos personales con la entrada en plena vigencia de la Ley Orgánica de Protección de Datos Personales (LOPDP) y la creación de la Superintendencia de Protección de Datos Personales. Antes de este avance, el país contaba únicamente con la garantía jurisdiccional del Hábeas Data[88] como mecanismo para enfrentar vulneraciones al derecho a la privacidad.[89] Sin embargo, este recurso es de carácter reactivo y limitado, ya que no previene violaciones, sino que se activa una vez que han ocurrido. Además, sus sentencias no tienen efectos generales, lo que dificulta la generación de criterios uniformes en la protección de datos personales. Así, la existencia de un organismo especializado, como la Superintendencia, representa un avance fundamental, pues permite desarrollar políticas preventivas, establecer estándares claros y garantizar una protección más efectiva de la autodeterminación informativa.

No obstante, se dispone de jurisprudencia que ha establecido criterios sobre el derecho a la protección de datos personales reconocido en el numeral 19 del artículo 66 de la Constitución. En la sentencia No. 2064-14/EP21[90] la Corte Constitucional del

---

[85] 1) Gobernanza de ciberseguridad; 2) Sistemas de información y gestión de incidentes; 3) Protección de servicios e infraestructuras críticas digitales; 4) Soberanía y defensa; 5) Seguridad pública y ciudadana; 6) Diplomacia en el ciberespacio y cooperación internacional; 7) Cultura y educación de ciberseguridad; ibíd., 2.

[86] Ecuador, *Ley Orgánica para la Trasformación Digital y Audiovisual*, art. 3.

[87] Ibíd., art. 1.

[88] El artículo 92 de la Constitución ecuatoriana reconoce esta figura, y menciona que toda persona tiene derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, personales y/o informes que se tengan de esta o sobre sus bienes que consten en entidades públicas o privadas en cualquier tipo de soporte, asimismo, tendrá derecho a conocer el uso que se ha hecho de esto, su propósito, el origen, destino de la información y el tiempo de vigencia del banco de datos, pudiendo solicitar su actualización, rectificación, eliminación o anulación. En Ecuador, *Constitución de la República del Ecuador*, Registro Oficial 449, 20 de octubre de 2008, art. 92.

[89] La revelación ilegal de base de datos es un delito contemplado en el artículo 229 del Código Orgánico Integral Penal, que se encuentra dentro de los delitos contra la seguridad de los activos de los sistemas de información y comunicación; sin embargo, esta problemática no se puede reducir a un delito debido a que tiene varias entradas que superan el ámbito penal, como es la de derechos humanos.

[90] En esta sentencia se analiza si existe vulneración del derecho constitucional al debido proceso en la garantía a recurrir el fallo y a la motivación, al principio de non reformatium in pejus, al derecho a la defensa; y, a la tutela judicial efectiva en la sentencia de segundo nivel, misma que resolvió revocar la decisión de primer nivel y declaró sin lugar la acción de hábeas data planteada en contra de una persona natural que poseía fotografías íntimas y personales de la actora. La Corte decide entrar al mérito del caso y

Ecuador[91] realiza un análisis referente al artículo 66 numeral 19 de la Constitución cuya conclusión se encuentra en siguiente párrafo:

> 104. Con base en ello, se puede llegar a una primera puntualización respecto a este tipo de manifestación de voluntad, esta requiere ser libre, específica, informada e inequívoca. Por consiguiente, que aquella sea libre, implica que la misma no esté sujeta a algún tipo de vicio del consentimiento, como la fuerza, la coerción o cualquier tipo de presión que se pueda ejercer sobre el titular, con el fin de que aquel preste su consentimiento. El requisito de especificidad implica que haya claridad en cuanto al tipo de tratamiento que autoriza el titular y el dato personal sobre el cual lo autoriza, así como a los sujetos que pueden realizar el tratamiento sobre los datos personales. Es decir, que la manifestación de voluntad exprese concretamente el o los tipos de tratamiento que se autorizan y específicamente con respecto a qué dato personal del titular se está autorizando dicho uso, así como el sujeto o los sujetos autorizados a realizar dicho tratamiento a los datos personales del titular. En cuanto al requisito de que el consentimiento sea inequívoco, ello está vinculado a la especificidad y claridad e implica que la manifestación de voluntad no sea ambigua, esto es, que no dé lugar a dudas respecto del consentimiento en sí mismo y su alcance.[92]

Así es como la Corte Constitucional del Ecuador deja claro que, para recolectar, archivar, procesar, distribuir o difundir datos personales se requiere de la autorización del titular o el mandato de la ley, y que esta autorización debe ser libre, específica, informada e inequívoca.

Por otro lado, desde marzo de 2023 entró en vigencia la "Ley Orgánica Reformatoria a varios Cuerpos Legales para el Fortalecimiento de las Capacidades Institucionales y la Seguridad Integral", que modifica varias partes del Código Orgánico Integral Penal (COIP) y otras leyes enfocadas en la seguridad pública y la inteligencia. Uno de los temas más preocupantes de este cuerpo legal es la creación de "agentes informáticos encubiertos"; esto afecta negativamente a la privacidad y la protección de datos en el país, pues se les otorga la capacidad de infiltrarse en plataformas informáticas, realizar seguimientos, vigilar y realizar compras controladas, lo que implica intrusión en la vida privada de las personas.[93] Asimismo, esta medida permite la recolección de

---

encuentra que hubo violación al derecho a la protección de datos personales y autodeterminación informativa, a la imagen, a la honra y buen nombre e intimidad. En Corte Constitucional del Ecuador, "Caso No. 2064-14-EP/21", Sentencia No. 2064-14-EP/21 § (2021).

[91] Corte Constitucional del Ecuador, "Sentencia No. 2064-14-EP/21 § (2021)", *Caso No. 2064-14-EP/21*.

[92] Ecuador Corte Constitucional del Ecuador, *Sentencia No. 2064-14-EP/21*, 27 de enero de 2021, 28.

[93] Ecuador, *Ley Orgánica Reformatoria a varios Cuerpos Legales para el Fortalecimiento de las Capacidades Institucionales y la Seguridad Integral*, Registro Oficial 279, Suplemento, 29 de marzo de 2023, art. 77.

información personal sin suficientes salvaguardias para la privacidad de las personas.[94] Además, estos agentes pueden intercambiar y enviar archivos con contenido ilícito, así como aplicar técnicas para preservar y descifrar información recolectada,[95] lo que pone en riesgo la confidencialidad y la integridad de los datos personales.

La creación de estos agentes va en contra de los principios de legalidad y proporcionalidad que deberían regir las políticas de vigilancia.[96] Además, no se ha garantizado un proceso adecuado de discusión y participación de las partes interesadas, lo que genera preocupación sobre la falta de transparencia y control en el uso de estas herramientas Al respecto, el último Examen Periódico Universal (EPU) llama al Ecuador a abstenerse de utilizar tecnologías de vigilancia y reconocimiento facial o biométrico que no cumplan con los estándares y obligaciones internacionales, así como regular la venta, la transferencia, el uso y la exportación de estas tecnologías."[97]

En conclusión, la situación actual del derecho a la protección de datos personales en el Ecuador ha estado marcada por un enfoque empresarial. Sin embargo, con la entrada en plena vigencia de la LOPDP y el inicio de actividades de la Superintendencia de Protección de Datos Personales, el país ha dado un paso importante hacia una regulación más efectiva. Sin embargo, persisten desafíos, ya que existen otras normas que, al aplicarse, pueden generar conflictos con la protección de datos personales, lo que resalta la necesidad de un marco normativo coherente y garantista.

### 2.3. Análisis comparado entre la Ley Orgánica de Protección de Datos Personales del Ecuador y el Reglamento General de Protección de Datos de la Unión Europea

La LOPDP guarda gran influencia con el RGPD de la UE, debido a que ésta normativa "ha transformado profundamente el enfoque global hacia la protección de datos, estableciendo un marco que ha sido adoptado, adaptado e interpretado de diversas maneras en diferentes jurisdicciones".[98] Este proceso, conocido como "Efecto Bruselas",

---

[94] De Souza Michel, "Ecuador: Muchos cambios, poco que celebrar", *Derechos Digitales*, 12 de mayo de 2023, 6, https://www.derechosdigitales.org/20752/ecuador-muchos-cambios-poco-que-celebrar/.

[95] Ecuador, *Ley Orgánica Reformatoria a varios Cuerpos Legales para el Fortalecimiento de las Capacidades Institucionales y la Seguridad Integral*, art. 77.

[96] Ibíd., 6.

[97] Derechos Digitales América Latina, "Contribuciones sobre derechos humanos en el entorno digital en Ecuador", 2022, 14.

[98] Diego Marcelo Bonilla-Morejón y Delia Paulina Samaniego-Quiguiri, «Evolución y desafíos de la protección de datos personales en el contexto de la globalización», *Horizon Nexus Journal* 2, n.º 1 (31 de enero de 2024): 65, doi:10.70881/hnj/v2/n1/34.

demuestra cómo las regulaciones de UE se convierten en estándares globales, pues, al ser uno de los mercados más grandes y estrictos del mundo, establece normativas que muchas empresas internacionales incorporan para poder operar en su territorio.[99]

La LOPDP tiene como fin regular el ejercicio del derecho a la protección de datos personales, autodeterminación informativa y demás derechos digitales, y aplica a los datos personales contenidos en cualquier soporte.[100] Así, el artículo 1 del RGPD "establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos"; así, deja claro que el Reglamento protege únicamente a las personas físicas con respecto a su derecho a la protección de datos personales, igual que la LOPDP.

La LOPDP define al "dato personal" como aquel "dato que identifica o hace identificable a una persona natural, directa o indirectamente".[101] El RGPD lo define de manera similar en el primer numeral del artículo 4, al mencionar que es "toda información sobre una persona física identificada o identificable", dejando claro que una persona es identificable mediante un identificador, que puede ser un nombre, un número de identificación, localización, identidad fisiológica, genética, económica, entre otros.

Ambos instrumentos también definen categorías especiales de datos personales como son los datos sensibles. En el RGPD se menciona que, salvo ciertas excepciones, esta prohibido el tratamiento de datos que revelen , entre otros, el origen étnico o racial, datos relativos a la salud o datos relativos a la vida sexual de una persona.[102] La LOPDP señala que los datos sensibles son los relativos a la "etnia, identidad de género, identidad cultural, religión, ideología, filiación política, pasado judicial, condición migratoria… y aquellos cuyo tratamiento indebido pueda dar origen a discriminación, atenten o puedan atentar contra los derechos y libertades fundamentales". Es claro como estos instrumentos consideran que existen datos que se deben considerar de manera especial, debido a que podrían condicionar los derechos y libertades fundamentales de las personas.

Por otra parte, tanto el RGPD como la LOPDP establecen que para proceder con el tratamiento y comunicación de datos personales es necesario el consentimiento,[103] que

---

[99] Ibíd, 66.

[100] Martínez et al., "La protección de datos personales en Ecuador", 376.

[101] Ecuador, *Ley Orgánica de Protección de Datos Personales*, art. 4.

[102] Parlamento Europeo y Consejo Europeo, *Reglamento General de Protección de Datos*, art. 9, num. 1.

[103] Salvo algunas excepciones como las establecidas en los arts. 7 y 36 de la LOPDP y en el art. 6 del RGPD.

se entiende como la "manifestación de la voluntad libre, específica, informada e inequívoca, por el que el titular de los datos personales autoriza al responsable del tratamiento de los datos personales a tratar los mismos".[104] Asimismo, en cualquier momento y sin ser necesario una justificación, se puede revocar el consentimiento, por lo que el responsable del tratamiento de datos debe establecer mecanismos para conseguirlo de forma sencilla y célere.[105] El artículo 7 del RGPD hace mención a que el consentimiento debe darse libremente (num. 4), que se puede retirar el consentimiento en cualquier momento (num. 3) y a la especificidad en su segundo numeral.

La LOPDP es aplicable si el tratamiento se realiza en territorio nacional, si el responsable o encargado del tratamiento de datos tiene domicilio en el Ecuador, o si el responsable o encargado del tratamiento que no se encuentra domiciliado en el Ecuador realiza el tratamiento de datos de personas que sí se encuentran en el Ecuador.[106] Este artículo claramente guarda estrecha relación con el artículo 3 del RGPD, que establece la misma aplicación Territorial para la UE.

Con respecto a los niños, niñas y adolescentes, la LOPDP,[107] su reglamento y el RGPD considera a las niñas, niños y adolescentes como personas incapaces, por lo que su consentimiento se debe obtener a través de sus representantes legales.[108] No obstante, de acuerdo con la LOPDP los adolescentes a partir de los 15 años de edad podrán otorgar su consentimiento (explícito) para el tratamiento de sus datos personales, siempre que se les especifique con claridad su fines;[109] mientras que en la UE una persona puede otorgar su consentimiento a partir de los 16 años.[110] Este consentimiento no puede menoscabar el interés superior de la niña, niño o adolescente, caso contrario, el consentimiento será inválido.

### 2.3.1. Gestión de riesgos y responsabilidad proactiva

---

[104] Ecuador, *Ley Orgánica de Protección de Datos Personales*, art. 4.

[105] Ibíd., art. 8.

[106] Ecuador, *Ley Orgánica de Protección de Datos Personales*, art. 3.

[107] Ibíd., art. 21.

[108] Ecuador, *Decreto Ejecutivo 904,* Registro Oficial 435, Suplemento, 13 de noviembre de 2023, art. 21; Parlamento Europeo y Consejo Europeo, Reglamento General de Protección de Datos, art. 8.1; De acuerdo con Gianclaudio Maglieri, los niños, niñas y adolescentes son el único grupo vulnerable reconocido en el RGPD. En Gianclaudio Malgieri, Vulnerability and Data Protection Law (United Kingdom: Oxford University Press, 2023), https://global.oup.com/academic/product/vulnerability-and-data-protection-law-9780192870339?cc=ec&lang=en&, 65.

[109] Ecuador, *Ley Orgánica de Protección de Datos Personales*, art. 24.

[110] Parlamento Europeo y Consejo Europeo, *Reglamento General de Protección de Datos*, art. 8.1.

De acuerdo con la extinta Directiva de Protección de Datos de la UE[111] y varios expertos en la materia, el RGPD (y por consecuencia la LOPDP), se fundamenta en la gestión de riegos.[112] Todas las responsabilidades de las empresas y los estados parten de este concepto, [113] utilizado en el sector de la seguridad de la información[114] y en el mundo empresarial. Sin embargo, ni el RGPD ni la LOPDP definen lo que debe entenderse por gestión de riesgos; no obstante, sí se señalan criterios, como los que se mencionan en el apartado 76 del RGPD:

> La probabilidad y la gravedad del riesgo para los derechos y libertades del interesado debe determinarse con referencia a la naturaleza, el alcance, el contexto y los fines del tratamiento de datos. El riesgo debe ponderarse sobre la base de una evaluación objetiva mediante la cual se determine si las operaciones de tratamiento de datos suponen un riesgo o si el riesgo es alto.[115]

De lo citado también se destaca que se mide el riesgo en función de los derechos y libertades del interesado, como también lo indica el segundo inciso del artículo 41 de la LOPDP.[116] De la misma manera, en el artículo 40 de la LOPDP se establece que para

---

[111] El Grupo de Trabajo del Artículo 29 era un organismo consultivo independiente de la Unión Europea, creado en virtud del artículo 29 de la Directiva 95/46/CE, también conocida como la Directiva de Protección de Datos de la UE, adoptada en 1995. Este grupo tenía como objetivo principal proporcionar asesoramiento experto sobre cuestiones relacionadas con la protección de datos y la privacidad, y garantizar la aplicación coherente de la normativa de protección de datos en todos los Estados miembros de la UE. Con la entrada en vigor del RGPD en 2018, el GT29 fue reemplazado por el Comité Europeo de Protección de Datos (CEPD). Este nuevo organismo asumió las responsabilidades del GT29 y fortaleció la cooperación entre las autoridades de protección de datos de la UE, proporcionando un marco más robusto y unificado para la protección de datos en toda la región. El CEPD tiene un mandato más amplio y vinculante en comparación con el GT29, lo que le permite emitir decisiones que deben ser acatadas por todas las autoridades nacionales de protección de datos. "Legado: Grupo de Trabajo del art. 29 | European Data Protection Board", accedido 14 de agosto de 2024, https://www.edpb.europa.eu/about-edpb/who-we-are/legacy-art-29-working-party_es, 1.

[112] Article 29 Data Protection Working Party, "Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679", 4 de abril de 2017, 29, https://ec.europa.eu/newsroom/document.cfm?doc_id=44137, 15.; Raphaël Gellert, The Risk-Based Approach to Data Protection (Oxford: Oxford Scholarship Online, 2020), https://doi.org/10.1093/oso/9780198837718.001.0001, 175.

[113] El RGPD hace referencia al término "riesgo" en setenta y tres ocasiones a lo largo del texto, y de forma específica en los artículos 4.24, 23.2.g, 24.1, 25.1, 27.2.a, 30.5, 32, 33, 34, 35, 36, 29.2, 49.1, entre otros.

[114] Enríquez Álvarez, "La Visión de América Latina sobre el Reglamento General de Protección de Datos", 102.

[115] Parlamento Europeo y Consejo Europeo, Reglamento General de Protección de Datos, párr. 76.

[116] El responsable y el encargado del tratamiento de datos personales deberán tomar las medidas adecuadas y necesarias, de forma permanente y continua, para evaluar, prevenir, impedir, reducir, mitigar y controlar los riesgos, amenazas y vulnerabilidades, incluidas las que conllevan un alto riesgo para los derechos y libertades del titular, de conformidad con la normativa que emita la Autoridad de Protección de Datos Personales. Ecuador, *Ley Orgánica de Protección de Datos Personales*, Registro Oficial 459, Suplemento, 26 de mayo de 2021, art. 41.

analizar el riesgo, amenazas y vulnerabilidades se debe aplicar una metodología que considere las particularidades del tratamiento, de las partes involucradas, las categorías y el volumen de datos personales.[117]

Ahora bien, el Comité Europeo de Protección de Datos ha desarrollado el documento "Directrices sobre la evaluación de impacto[118] relativa a la protección de datos (EIPD) y para determinar si el tratamiento entraña probablemente un alto riesgo a efectos del Reglamento (UE) 2016/679" (Directrices WP248), donde se definen los conceptos de "riesgo" y "gestión del riesgo".

El primero es definido como un "escenario que describe un acontecimiento y sus consecuencias estimado en términos de gravedad y probabilidad"[119], mientras que el segundo se define como "las actividades coordinadas para dirigir y controlar una organización respecto al riesgo".[120] Por lo tanto, la gestión de riesgos es un proceso que consiste en identificar, analizar y tratar los posibles efectos adversos o no previstos que el tratamiento de datos personales pueda tener para los derechos y libertades de las personas interesadas. La gestión de riesgos debe permitir que la persona responsable o encargada del tratamiento adopte las medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad apropiado al riesgo.

Asimismo, la gestión de riegos implica observar varios principios. El de confidencialidad, que implica prevenir el uso no autorizado de los datos; el principio de integridad, que conlleva a prevenir que los datos se cambien sin autorización; el principio de disponibilidad, que consiste en garantizar el acceso a los datos; el principio de trazabilidad, que consiste en el registro de acciones efectuadas en el tratamiento de los datos, que suele servir para las auditorías; y el principio de resiliencia, entendido como la capacidad de un sistema informático para resistir ataques.[121]

---

[117] Ibíd., art. 40.

[118] El artículo 42 de la LOPDP sobre la evaluación de impacto del tratamiento de datos personales indica que se debe hacer una evaluación de impacto cuando se haya identificado la probabilidad que el tratamiento de datos pueda conllevar a un alto riesgo para los derechos y libertades del titular, como en la evaluación sistemática y exhaustiva que se base en un tratamiento automatizado, en el tratamiento a gran escala de las categorías especiales de datos o en la observación sistemática a gran escala de una zona de acceso público. Ibíd., art. 42.

[119] Grupo "Protección De Datos" Del Artículo 29, "Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento "entraña probablemente un alto riesgo" a efectos del Reglamento (UE) 2016/679", *AEPD*, 4 de octubre de 2019, 7, https://www.aepd.es/sites/default/files/2019-09/wp248rev01-es.pdf.

[120] Ibíd.

[121] Tradicionalmente se han señalado exclusivamente los tres primeros principios. Enríquez Álvarez, "La Visión de América Latina sobre el Reglamento General de Protección de Datos", 103.

Por otro lado, la gestión de riesgos se encuentra estrechamente relacionado con el principio de responsabilidad proactiva, también conocido como *accountability*.[122] Para el RGPD, este principio implica tener la capacidad de demostrar que los datos personales son tratados de manera lícita, recogidos con fines determinados, explícitos y legítimos, adecuados con los fines para los que son tratados, que sean exactos, mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario y tratados de manera que se garantice una seguridad adecuada.[123]

La LOPDP define a la responsabilidad proactiva como la debida implementación de mecanismos para la protección de datos personales, para lo que podrá valerse de estándares, mejores prácticas, esquemas de regulación, entre otros, con el fin de rendir cuentas sobre el tratamiento de datos personales.[124] La norma dedica todo el octavo capítulo a este principio, indicando que los responsables y encargados pueden adherirse a códigos de conducta, certificaciones, sellos, marcas de protección y similares, sin que esto implique eximir de la responsabilidad de cumplir con las disposiciones de la ley.[125] Para esto, la Superintendencia de Protección de Datos debe promover la elaboración de códigos de conducta por sectores, tomando en cuenta las necesidades específicas de cada uno.

Así, el principio de responsabilidad proactiva en el RGPD y en la LOPDP comparten similitudes en su objetivo de garantizar la protección adecuada de los datos personales y fomentar la rendición de cuentas por parte de los responsables del tratamiento. Ambos principios requieren que las organizaciones implementen medidas para proteger los datos, como la adopción de estándares, mejores prácticas y la demostración de cumplimiento. Además, ambas normativas reconocen la importancia de la transparencia y la precisión en el tratamiento de datos, así como la necesidad de no mantenerlos por más tiempo del necesario.

Por lo tanto, la responsabilidad proactiva es una manera de aplicar el derecho a la protección de datos personales, que busca prevenir y anticipar los problemas jurídicos antes de que se produzcan, mediante el uso de herramientas como la gestión de riesgos,

---

[122] Katerina Demetzou, "GDPR and the Concept of Risk: The Role of Risk, the Scope of Risk and the Technology Involved", en *Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data*, ed. Eleni Kosta et al., vol. 547, IFIP Advances in Information and Communication Technology (Cham: Springer International Publishing, 2019), 137-54, doi:10.1007/978-3-030-16744-8_10, 141.

[123] Parlamento Europeo y Consejo Europeo, Reglamento General de Protección de Datos, art. 5.

[124] Ecuador, *Ley Orgánica de Protección de Datos Personales*, art. 10.

[125] Ibíd., art. 52.

la evaluación de impacto, la privacidad por diseño, la transparencia, la rendición de cuentas y la participación de las partes interesadas.

### 2.4. Responsabilidades exclusivas del Estado ecuatoriano frente a la protección de datos personales

El RGPD y la LOPDP establecen obligaciones para el responsable y el encargado de la protección de datos, que pueden ser Estados o empresas. Sin embargo, existen responsabilidades exclusivas para los Estados, que se desarrollarán en el presente subtítulo.

El RGPD establece varias responsabilidades a los Estados miembros de la Unión Europea en relación con la protección de datos, y las establece principalmente en su capítulo sexto (Autoridades de control independientes) y séptimo (cooperación y coherencia). Con el propósito de garantizar el derecho a la protección de datos personales, el artículo 51 ordena a cada Estado parte designar una o varias autoridades públicas de control, que deben ser independientes para poder supervisar y hacer cumplir el RGPD.[126] Estas autoridades deben notificar a la Comisión las disposiciones legales que adopten,[127] llevar a cabo auditorias de cumplimiento,[128] abordar las reclamaciones de los interesados[129] y, cuando sea necesario, emitir multas por incumplimiento del RGPD,[130] entre otras funciones.

Este reglamento también incorpora deberes de desarrollar progresivamente la protección de datos personales. Por ejemplo, señala que las autoridades de control son responsables de asesorar al Parlamento nacional, al Gobierno y a otras instituciones y organismos sobre las medidas legislativas y administrativas relativas a la protección de datos personales.[131]

El séptimo capítulo del reglamento se centra en la cooperación y coherencia entre las autoridades de protección de datos de los Estados miembros de la UE. Este capítulo es crucial para garantizar una aplicación uniforme y coherente del RGPD en toda la UE. A continuación, se detallan los principales elementos de este capítulo:

---

[126] Ibíd., art. 52.
[127] Ibíd., art. 51.2.
[128] Ibíd., art. 58.1. b.
[129] Ibíd., art. 57.1. f.
[130] Ibíd., art. 58.2. i.
[131] Ibíd., art. 57.1. c.

1 Artículo 60 - Cooperación entre la autoridad de control principal y las autoridades de control interesadas: Este artículo establece la obligación de la autoridad de control principal (la autoridad de control del Estado miembro donde una empresa tiene su establecimiento principal en la UE) de cooperar con otras autoridades de control interesadas en casos que involucren el tratamiento transfronterizo de datos.
2 Artículo 62 Operaciones conjuntas de las autoridades de control: Establece que las autoridades de control deben proporcionarse mutuamente asistencia y cooperación, incluida la facilitación de investigaciones y la recopilación de pruebas.
3 Artículo 63 Mecanismo de coherencia: Se refiere a la aplicación coherente del Reglamento, por lo que las autoridades de control cooperarán entre sí y con la Comisión, de modo que se aplique el RGPD de manera homogénea en todos los Estados parte.
4 Artículo 67 Intercambio de información: Establece la obligación de las autoridades de control de intercambiar información relevante entre sí.
5 Artículo 68 Comité Europeo de Protección de Datos: Este artículo establece la creación de un Comité Europeo de Protección de Datos (CEPD) compuesto por representantes de las autoridades de control de cada Estado miembro y del Supervisor Europeo de Protección de Datos. El CEPD tiene la tarea de contribuir a la coherencia en la aplicación del RGPD.[132]

El séptimo capítulo destaca la importancia de la cooperación y la coherencia entre las autoridades de protección de datos de la UE para garantizar un enfoque armónico en la aplicación del RGPD en casos de tratamiento transfronterizo de datos personales. Esto contribuye a fortalecer la protección de los derechos de privacidad de los ciudadanos de la UE y a garantizar un marco regulatorio coherente en toda la Unión.

Por su parte, la LOPDP establece una "Autoridad de Datos Personales" en su capítulo XII, y la define como el " órgano de control y vigilancia encargado de garantizar a todos los ciudadanos la protección de sus datos personales, y de realizar todas las acciones necesarias para que se respeten los principios, derechos, garantías y procedimientos previstos en la presente Ley […]".[133] Esta autoridad, que es el

[132] Ibíd., art. 70.1.
[133] Ecuador, *Ley Orgánica de Protección de Datos Personales*, art. 76.

Superintendente de Protección de Datos, tiene entre sus funciones supervisar las actividades del responsable y del encargado del tratamiento de datos personales, ejercer la potestad sancionadora, resolver reclamos, realizar auditorías, administrar el Registro Nacional de Protección de Datos Personales, atender consultas, promover el ejercicio del derecho a la protección de datos personales, entre otros.[134]

Para profundizar sobre las responsabilidades que conlleva el derecho a la privacidad por medio de la protección de datos personales, diferentes comités también han publicado Observaciones Generales (OG). Por ejemplo, el Comité de Derechos Humanos (CDH), que supervisa la aplicación de los derechos civiles y políticos reconocidos en el PIDCP,[135] en su OG 16 manifiesta que las obligaciones impuestas por el artículo 17 del PIDCP exigen que el Estado se abstenga de injerencias incompatibles con el artículo mencionado y que adopte un marco legislativo que regulen las injerencias autorizadas en la vida privada, así como la recopilación y el registro de información personal en computadoras, bancos de datos u otros dispositivos, tanto por las autoridades públicas como por las particulares o entidades privadas, y que se proporcionen recursos eficaces contra los responsables de esas injerencias.[136] También aclara algunos términos del artículo, como el de ilegalidad y arbitrariedad, pues menciona que pueden producirse injerencias arbitrarias incluso cuando estas se encuentren previstas en la ley, si estas no van conforme a las disposiciones, propósitos y objetivos de PIDCP.[137]

Otro punto importante que resaltar de esta OG es que establece que los Estados deben velar por que la información relativa a la vida privada de una persona nunca se la utilice para fines incompatibles con el PIDCP, y que debe prohibirse la vigilancia por medios electrónicos o de otra índole, por lo que toda persona debe tener el derecho de verificar qué autoridades públicas o qué organismos privados tienen su información personal, y si esos datos personales son incorrectos o se han compilado o elaborado en contravención de las disposiciones legales, se debe tener el derecho a pedir su rectificación o eliminación.[138] Estas disposiciones se deben considerar en el actual contexto, sin embargo cabe mencionar que esta OG fue publicada en 1988, es decir, hace

---

[134] Ibíd, art. 76.

[135] ACNUDH, *Comité de Derechos Humanos*, accedido 16 de septiembre de 2020, párr. 1, https://www.ohchr.org/SP/HRBodies/CCPR/Pages/CCPRIndex.aspx.

[136] Comité de Derechos Humanos, *Observación General Nro. 16. Derecho a la intimidad*, art. 17, párrs. 1-7- 9-10-11, 1988.

[137] Ibíd., párrs. 3-4.

[138] Ibíd., párrs. 8-10.

más de tres décadas, por lo que evidentemente se encuentra desactualizada considerando los abismales avances de la tecnología.

El Consejo de Derechos Humanos de la ONU a través del Alto Comisionado de las Naciones Unidas para los Derechos Humanos y del Relator Especial sobre el derecho a la privacidad ha desarrollado documentos actualizados sobre el derecho a la privacidad, donde menciona que este derecho abarca también los metadatos, ya que al analizarse y reunirse pueden conocer del comportamiento, relaciones sociales, preferencias e identidad de una persona,[139] sin embargo, al no ser instrumentos normativos resulta más complicado que los Estados partes los consideren.

En la misma línea, el informe anual del Alto Comisionado de 2018 denominado "El derecho a la privacidad en la era digital", manifiesta que "la privacidad puede entenderse como la presunción de que el individuo debe tener una esfera de desarrollo autónomo, interacción y libertad, una 'esfera privada' con o sin relación con otras y libre de la intervención del Estado y de la intervención excesiva no solicitada de otros individuos no invitados"[140]. Esto es importante porque significa que este derecho no solo se encuentra comprometido cuando la información de la persona es utilizada por un ser humano o un algoritmo, sino que se vulnera el derecho a la privacidad con la simple recolección de datos relativos a la identidad, la familia o la vida de una persona,[141] pues a través de esas acciones, se pierde el control sobre una información que podría poner en riesgo la vida privada.

Se debe considerar también al Informe de 2019 presentado al Consejo de Derechos Humanos del Relator Especial sobre el derecho a la privacidad de Naciones Unidas, Joseph Cannataci,[142] que establece principios para garantizar el derecho a la privacidad, como el de limitación de la finalidad, que implica que especialmente con los datos médicos el uso secundario de los datos personales debe ser compatible con los fines iniciales, o el principio de "si es intercambiable, es supervisable" para así proteger toda

---

[139] ONU Consejo de Derechos Humanos, "El derecho a la privacidad en la era digital", 3 de agosto de 2018, párr. 6, A/HRC/39/29.

[140] Ibíd., párr. 5.

[141] Ibíd., párr. 7.

[142] En 2015 el Consejo de Derechos Humanos nombró a Joseph Cannataci como el primer Relator Especial sobre el derecho a la privacidad. Este tiene entre sus funciones, según la Resolución 28/16 del Consejo de Derechos Humanos, concienciar sobre la importancia de proteger y promover el derecho a la privacidad en relación con los retos que ofrece la era digital, así como denunciar las presuntas violaciones de este derecho reconocido en la DUDH y el PIDCP. En ACNUDH, "Relator Especial sobre el derecho a la privacidad", accedido 17 de septiembre de 2020, Párrs.2-8-10, https://www.ohchr.org/SP/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx.

la información personal que se intercambia a nivel nacional e internacional.[143] Este derecho también debe interpretarse bajo los principios de legalidad, necesidad y proporcionalidad, y a menudo actúa como puerta de acceso al disfrute de la libertad de opinión y expresión.[144]

Así es cómo se pueden observar los esfuerzos que existen desde el ámbito internacional para regular este nuevo fenómeno, pero es evidente que hace falta normativa mucho más sólida y actualizada que los Estados se encuentren obligados a observar para garantizar el derecho a la privacidad en la web. Por otro lado, se debe reconocer que el nuevo modelo de negocio basado en la extracción masiva de datos parte mayoritariamente de las empresas privadas millonarias como *Google* o *Meta*, que poseen más poder que la mayoría de Estados del mundo, por lo que es ilusorio considerar que todos los Estados, especialmente los que poseen instituciones débiles, puedan garantizar por sí solos los derechos de sus ciudadanos en la red.

### 2.5.Responsabilidad de las empresas

El RGPD establece responsabilidades a empresas en relación con la recopilación, almacenamiento y gestión de datos personales. Estas obligaciones se aplican tanto a las organizaciones europeas que tratan datos personales de ciudadanos en la UE como a las organizaciones que tienen su sede fuera de la UE pero tratan datos personales relacionados con ofertas de bienes o servicios a ciudadanos en la UE o supervisan el comportamiento de ciudadanos en la UE (aplicación extraterritorial).[145] A continuación, se detallan algunas de las principales obligaciones según el RGPD:

1 Responsabilidad proactiva (rendición de cuentas): Las organizaciones deben demostrar que cumplen con el RGPD y todas las obligaciones aplicables. Esto implica llevar a cabo evaluaciones de impacto de protección de datos, mantener registros de actividades de procesamiento y cooperar con las autoridades de protección de datos cuando sea necesario.[146]

---

[143] ONU Consejo de Derechos Humanos, "Informe del Relator Especial sobre el Derecho a la Privacidad", 16 de octubre de 2019, Párrs. 46-122, A/HRC/40/63.

[144] ONU Asamblea General, "Promoción y protección del derecho a la libertad de opinión y expresión. Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión", 29 de agosto de 2018, párr. 33, A/73/348*.

[145] Parlamento Europeo y Consejo Europeo, Reglamento General de Protección de Datos, art. 3.

[146] Ibíd., art. 5.2.

2 Licitud del tratamiento: Se centra en las bases legales para el tratamiento de datos personales, estableciendo que el procesamiento debe basarse en el consentimiento, la ejecución de un contrato, el cumplimiento de una obligación legal, la protección de intereses vitales, la tarea realizada en interés público o el ejercicio de autoridad oficial, o los intereses legítimos perseguidos por el responsable o un tercero.[147]

3 Deber de informar: Las empresas deben proporcionar información clara y transparente a los interesados sobre cómo se tratan sus datos personales. Esto incluye detalles sobre el propósito del tratamiento, la base legal, los derechos del interesado y otros aspectos relevantes.[148]

4 Derecho al olvido (derecho de supresión): Establece el derecho de los individuos a solicitar la supresión de sus datos personales, y obliga a las empresas a cumplir con esta solicitud en ciertas circunstancias.[149]

5 Protección de datos desde el diseño y por defecto: Las empresas deben considerar la privacidad desde el inicio al diseñar productos, servicios o sistemas que involucren el procesamiento de datos personales. Además, deben implementar medidas técnicas y organizativas para garantizar la protección adecuada de los datos.[150]

6 Registros de actividades de tratamiento: Obliga a las empresas a mantener registros internos de sus actividades de procesamiento de datos.[151]

7 Seguridad del tratamiento: establece la obligación de implementar medidas de seguridad adecuadas para proteger los datos personales.[152]

8 Evaluación de impacto relativa a la protección de datos: obliga a realizar evaluaciones de impacto cuando el tratamiento de datos pueda implicar un alto riesgo para los derechos y libertades de los individuos.[153]

9 Designación del Delegado de Protección de Datos (DPO): Cuando lo establezca el Reglamento, las organizaciones deben nombrar un DPO.[154] El

[147] Ibíd., art. 6.
[148] Ibíd., arts. 12, 13, 14.
[149] Ibíd., art. 17.
[150] Ibíd., art. 25.
[151] Ibíd., art. 30.
[152] Ibíd., art. 32.
[153] Ibíd., art. 35.
[154] Ibíd., art. 37.

> DPO es responsable de supervisar el tratamiento de datos personales dentro de la empresa y de asesorar a los empleados sobre sus obligaciones.[155]

Por su parte, la LOPDP en su capítulo VII regula al responsable, encargado y delegado de protección de datos personales, y en su capítulo VIII a la responsabilidad proactiva de las empresas. Así, el responsable del tratamiento de datos personales[156] debe regirse en apego a los principio y derechos desarrollados en la LOPDP, implementar requisitos y herramientas apropiadas para garantizar que el tratamiento se ha realizado de acuerdo a la norma, aplicar procesos de verificación, evaluación y valoración periódica, implementar políticas de protección de datos personales, utilizar metodologías de análisis y gestión de riesgos, así como prevenir y controlar los mismos, notificar al Superintendente de Protección de Datos y al titular si se ha vulnerado la seguridad de sus datos, implementar la protección de datos personales desde el diseño, entre otras funciones.[157]

La LOPDP también menciona que se debe designar un delegado de protección de datos personales cuando el tratamiento se lleve a cabo por el sector público, cuando las actividades del responsable o encargado requieran de un control permanente debido a su volumen, naturaleza, alcance o finalidades, si se refiere al tratamiento a gran escala de categorías especiales de datos, y cuando no se refiera a datos realizados con la seguridad nacional.[158] Entre las funciones del delegado de protección de datos personales se encuentra el asesorar sobre las disposiciones contenidas en la ley, su reglamento y conforme a las directrices emitidas por el Superintendente de Protección de Datos y supervisar su cumplimiento, asesorar en el análisis de riesgo, evaluación de impacto y de seguridad, cooperar con el Superintendente de Protección de Datos y las demás que llegase a establecer el mismo.

El informe de REDESCA de 2019 sobre empresas y Derechos Humanos posee una sección específica en la que resalta la responsabilidad de los Estados de regular las actividades empresariales, como servicios en línea, *big data* y cibervigilancia,[159] e

---

[155] Ibíd., art. 39.

[156] El encargado de tratamiento de datos personales tendrá las mismas obligaciones que el responsable del tratamiento de datos personales en lo que le sea aplicable. Ecuador, *Ley Orgánica de Protección de Datos Personales*, Registro Oficial 459, Suplemento, 26 de mayo de 2021, art. 47.

[157] Ibíd.

[158] Ibíd., art. 48.

[159] Comisión Interamericana de Derechos Humanos, "CIDH/REDESCA/INF.1/19", párr. 268.

identifica como campo potencialmente riesgoso a la intimidad y protección de datos, así como la explotación de datos con fines electorales.[160] También impone obligaciones positivas a las empresas, como el de crear un entorno en el que se respeten los derechos humanos, a través de la implementación de sistemas eficaces de supervisión, evaluaciones de impacto en los derechos y sistemas de denuncias por los daños de sus actividades, bajo los principios orientadores de transparencia, no discriminación, privacidad, pluralismo, igualdad y neutralidad de la red.[161]

Por otro lado, es necesario la cooperación de las empresas, y para este fin se han desarrollado los Principios Rectores sobre las Empresas y los Derechos Humanos de las Naciones Unidas[162] -PRNU-, también conocidos como principios de Ruggie.[163] Este instrumento consiste en 31 principios distribuidos en 3 capítulos para implementar el marco de proteger, respetar y remediar, para así prevenir y reparar la violación de derechos humanos relacionados con la actividad empresarial. Estos 3 capítulos se refieren al deber del Estado de proteger los derechos humanos, a la responsabilidad de las empresas de respetar los derechos humanos y al acceso a mecanismos de reparación.

El PRNU sostiene que las empresas tienen la responsabilidad de respetar los derechos humanos, que incluye la obligación de "abstenerse de infringir los derechos de terceros y hacer frente a las consecuencias negativas sobre los derechos humanos en las que tengan alguna participación".[164] Además, deben actuar con debida diligencia, esto implica que para identificar, prevenir, mitigar y responder por las consecuencias negativas en los derechos humanos, todas las actividades de las empresas deben incluir una evaluación del impacto real y potencial sobre estos, la integración de conclusiones y la actuación al respecto, y el seguimiento de las respuestas, bajo una comunicación adecuada.[165]

En lo que respecta al Sistema Interamericano de Derechos Humanos (SIDH), el Comité Jurídico Interamericano en 2014 formuló la "Guía de Principios sobre Responsabilidad Social de las Empresas en el Campo de los Derechos Humanos y el

---

[160] Ibíd., párr. 275.

[161] Ibíd., párrs. 272-273-285.

[162] ONU Consejo de Derechos Humanos, "Informe del Relator Especial sobre el Derecho a la Privacidad", párr. 109.

[163] Debido a que fueron publicados por John Ruggie cuando fungía de Representante Especial del Secretario General de la ONU sobre la cuestión de los derechos humanos y las empresas transnacionales.

[164] ONU Consejo de Derechos Humanos, "Principios Rectores sobre las Empresas y los Derechos Humanos", 15 de junio de 2011, P.11, HR/PUB/11/04.

[165] Ibíd., 17.

Medio Ambiente en las Américas", donde se refiere a orientaciones de responsabilidad compartida y acciones para empresas tendientes a proteger los derechos. En 2017 publicó el informe sobre la "Regulación Consciente y Efectiva de las Empresas en el Ámbito de los Derechos Humanos", donde se propone avanzar en la regulación consiente y efectiva de las empresas,[166] y en 2019 La Comisión Interamericana de Derechos Humanos (CIDH) ha publicado un Informe del Relator Especial sobre Derechos Económicos, Sociales, Culturales y Ambientales (REDESCA) en el que parte de la base de las obligaciones internacionales de los Estados en materia de derechos humanos en supuestos en los que actividades empresariales se encuentren involucradas con la realización o afectación de derechos.[167]Asimismo, todos sus órganos han reconocido en diferentes casos que "puede generarse responsabilidad internacional del Estado en relación con actos cometidos por empresas que hayan involucrado la afectación a los derechos humanos".[168]

Así, el informe de 2019 de REDESCA afirma que los principios contenidos en el PRNU deben entenderse como un todo coherente, de manera que las medidas adoptadas por los Estados con respecto a la protección deberían generar efectos en el comportamiento de las empresas que tienen la obligación de respeto, y estos a su vez relacionarse con el acceso a mecanismos de reparación efectiva.[169] También se establece que el PRNU es la base conceptual mínima, dinámica y evolutiva de referencia de gobernanza mundial en la materia, por lo tanto, los Principios Rectores de Naciones Unidas son una fuente autorizada para aplicarse en el sistema interamericano de derechos humanos.[170]

Es claro que la era digital ha traído nuevos desafíos y riesgos para los derechos humanos, y han aumentado los casos de vulneraciones a los derechos producto de la actividad empresarial.[171] La responsabilidad de las empresas en el manejo y protección

---

[166] Comisión Interamericana de Derechos Humanos, "Informe Empresas y Derechos Humanos: Estándares Interamericanos", 1 de noviembre de 2019, párr. 16, CIDH/REDESCA/INF.1/19.

[167] Ibíd., párr. 25.

[168] Por ejemplo, en el "Informe sobre la situación de los Derechos Humanos en Ecuador" de 1997, la CIDH incitó al Estado a tomar medidas para evitar daños a las personas afectadas debido al comportamiento de los concesionarios y actores privados alrededor de la explotación petrolera; o la Corte Interamericana de Derechos Humanos en la Opinión Consultiva de 2003 sobre el principio de igualdad y no discriminación y los trabajadores migrantes, donde manifiesta que los Estados no deben permitir que los empleadores privados violen los derechos de los trabajadores migrantes. En Comisión Interamericana de Derechos Humanos, "Informe Empresas y Derechos Humanos: Estándares Interamericanos", 1 de noviembre de 2019, párr. 17-18-23, CIDH/REDESCA/INF.1/19.

[169] Ibíd., párr. 9.

[170] Ibíd., párrs. 10-11.

[171] Comisión Interamericana de Derechos Humanos, "CIDH/REDESCA/INF.1/19", párr. 12.

de los datos personales adquiere una dimensión aún más crítica cuando se trata de niños, niñas y adolescentes. Dado que estos grupos son especialmente vulnerables a la explotación digital y a los efectos negativos de la vigilancia y el uso indiscriminado de sus datos, es imperativo que las compañías implementen medidas robustas y transparentes dirigidas especialmente a los NNA. Solo mediante la aplicación rigurosa de evaluaciones de impacto, gestión de riesgos y estándares internacionales de protección, se podrá garantizar un entorno digital que salvaguarde la privacidad y promueva la salud mental y el desarrollo integral de las nuevas generaciones.

## 3. Contenido y alcance del derecho a la salud mental de niños, niñas y adolescentes a la luz de la protección de datos personales

El derecho a la salud es un derecho reconocido en varios instrumentos de derechos humanos, como en el artículo 12 del Pacto Internacional de Derechos Económicos Sociales y Culturales (PIDESC),[172] en el artículo 25 de la Declaración Universal de Derechos Humanos -DUDH-,[173] y en el artículo 24 de la Convención sobre los Derechos del Niño -CDN-.[174] Todos estos instrumentos coinciden en definir el derecho a la salud como la facultad de toda persona de poder disfrutar del más alto nivel posible de salud física y mental, por lo que los Estados deben adoptar medidas para garantizarlo. En la Constitución se encuentra reconocido en el artículo 32, que establece a la salud como un derecho fundamental de todas las personas, y señala las características que debe tener el sistema integral de salud, como el acceso universal, la igualdad, la calidad, la no discriminación y el enfoque intercultural, de género y generacional.[175] A continuación, se examinan los impactos que generan los entornos digitales en la salud mental de NNA y cómo se configura el derecho a la salud mental de niños, niñas y adolescentes frente a los desafíos y riesgos que presentan los entornos digitales.

---

[172] Los Estados Partes en el presente Pacto reconocen el derecho de toda persona al disfrute del más alto nivel posible de salud física y mental. Entre las medidas que deben adoptar los Estados se encuentra el sano desarrollo de los niños, el mejoramiento del medio ambiente y la creación de condiciones que aseguren a todos asistencia médica y servicios médicos en caso de enfermedad. En ONU Asamblea General, "PIDCP", art. 25

[173] "Toda persona tiene derecho a un nivel de vida adecuado que le asegure, así como a su familia, la salud y el bienestar, y en especial la alimentación, el vestido, la vivienda, la asistencia médica y los servicios sociales necesarios […]". En ONU Asamblea General, "DUDH", art. 12.

[174] Los Estados Partes reconocen el derecho el niño al disfrute del más alto nivel posible de salud y a servicios para el tratamiento de las enfermedades y la rehabilitación de la salud. Los Estados Partes se esforzarán por asegurar que ningún niño sea privado de su derecho al disfrute de esos servicios sanitarios. En ONU Asamblea General, "CRC", art. 24.

[175] Ecuador, *Constitución de la República del Ecuador*, art. 32.

### 3.1. Vulnerabilidades psicosociales en la infancia y adolescencia frente a al entorno digital

Los niños, niñas y adolescentes son un grupo vulnerable en entornos digitales por varias razones. Entre ellas, porque se encuentran en proceso de desarrollo cognitivo y emocional,[176] lo que los hace más susceptibles a los impactos negativos del uso excesivo de dispositivos digitales. Su capacidad para comprender y manejar adecuadamente la información que encuentran en línea puede ser limitada, lo que los hace más propensos a ser influenciados negativamente o a encontrarse con contenido inapropiado.[177]

Los niños, niñas y adolescentes son quienes presentan mayores grados de inseguridad, ansiedad y depresión mientras más tiempo se mantienen conectados a las redes sociales,[178] pues aún están aprendiendo a autorregular su comportamiento y sus emociones.[179] El acceso constante a dispositivos digitales puede dificultar este proceso, ya que pueden volverse dependientes de la gratificación instantánea que ofrecen los dispositivos, lo que puede llevar a problemas de adicción y dificultades para concentrarse en otras actividades importantes, como el estudio o la interacción social.[180]

Los niños, niñas y adolescentes están creciendo en una era en la que el uso de dispositivos digitales es omnipresente. Esto significa que están constantemente expuestos a mensajes publicitarios, redes sociales y otras formas de contenido digital que pueden influir en sus percepciones y comportamientos de manera negativa.[181] Varios estudios respaldan lo afirmado. Por ejemplo, el Fondo de las Naciones Unidas para la Infancia (UNICEF), ha reconocido que el uso excesivo o inapropiado de las nuevas tecnologías puede tener un impacto negativo en la salud mental de las personas.[182] Esto incluye, por ejemplo, el uso compulsivo de las redes sociales, el acoso en línea, exposición a

---

[176] Emilio Salao Sterckx, entrevistado por el autor, 22 de mayo de 2024.Para leer la entrevista completa, ver Anexo 1.

[177] Fernando Ocaña, entrevistado por el autor, 21 de mayo de 2024. Para leer la entrevista completa, ver Anexo 4.

[178] Miguel Escurra Mayaute y Edwin Salas Blas, "Construcción y validación del cuestionario de adicción a redes sociales", *Universidad Nacional Mayor de San Marcos, Perú. Universidad de San Martín de Porres, Perú*, 2014, 73–91, 74; Centre for Mental Health, "Impacto de las redes sociales sobre la salud mental de los niños, niñas y adolescentes, según el Centre for Mental Health", *InfoCop Online-Revista de Psicología*, 2018, 1-3, http://www.infocop.es/print.asp?print=yes.

[179] Emilia Piedra, entrevistada por el autor, 14 de mayo de 2024. Para leer la entrevista completa, ver Anexo 4.

[180] Henry Zaruma, entrevistado por el autor, 18 de mayo de 2024. Para leer la entrevista completa, ver Anexo 4.

[181] Anexo 4.

[182] Unicef, "Niños en un mundo Digital", 2017, www.unicef.org/SOWC2017., 4

información errónea o engañosa, afectación en la calidad del sueño y la regulación del estado de ánimo.[183]

En este sentido, estudios demuestran que la exposición temprana a la televisión y los medios digitales durante los primeros años de vida ha sido objeto de estudio debido a sus posibles efectos en el procesamiento sensorial de los NNA. Se ha observado que esta exposición se correlaciona con resultados atípicos en dicho procesamiento, lo que implica una alteración en la capacidad de los NNA para procesar adecuadamente el entorno que los rodea. Este fenómeno puede llevar a los infantes a desconectarse de la realidad, perder interés en actividades convencionales y buscar estímulos más intensos en su entorno, o sentirse abrumados frente a estímulos sensoriales como sonidos fuertes o luces brillantes.[184]

Investigaciones han revelado que, a los 12 meses de edad, la simple exposición a una pantalla se asocia con una probabilidad significativamente mayor (105%) de manifestar comportamientos sensoriales catalogados como “altos”, en contraposición a los considerados “típicos”. Además, a los 18 meses, cada hora adicional dedicada diariamente a la visualización de contenido frente a una pantalla se relaciona con un incremento del 23% en la probabilidad de exhibir comportamientos sensoriales “altos”, específicamente relacionados con la evitación de sensaciones y una baja capacidad de registro sensorial.[185] Estos hallazgos complementan una serie de resultados concernientes al tiempo dedicado a la exposición frente a pantallas en bebés, niñas y niños pequeños, entre los cuales se incluyen el retraso en el desarrollo del lenguaje, problemas conductuales, trastornos del sueño, dificultades de atención y demoras en la resolución de problemas.[186]

En el reportaje “ #FELIZ La dictadura de la felicidad de las redes sociales, se manifiesta que las redes sociales refuerzan la idea de una sociedad en la que las personas anhelan profundamente la felicidad, por lo que ese “algoritmo de la felicidad” está siendo

---

[183] Rodrigo Jácob Moreira de Freitas et al., “Percepciones de los adolescentes sobre el uso de las redes sociales y su influencia en la salud mental”, *Enfermería Global* 20, n.º 64 (2021): 324-64, doi:10.6018/eglobal.462631, 332.

[184] Karen Frankel Heffler et al., “Early-Life Digital Media Experiences and Development of Atypical Sensory Processing”, *JAMA Pediatrics* 178, n.º 3 (1 de marzo de 2024): 266, doi:10.1001/jamapediatrics.2023.5923, E2.

[185] Ibíd., E4.

[186] Ibíd; Yalda T. Uhls et al., "Five days at outdoor education camp without screens improves preteen skills with nonverbal emotion cues", *Computers in Human Behavior* 39 (1 de octubre de 2014): 387-92, doi:10.1016/j.chb.2014.05.036, 389.

creado y reforzado por las redes sociales.[187] De esta manera se replica lo que hace la publicidad: despertar deseo en otras personas, expresado a través de los *likes* en *Facebook,* o los corazones en *Instagram* y *TikTok*.

Las redes sociales han llegado a desempeñar un papel fundamental en la satisfacción del deseo de reconocimiento y pertenencia. La necesidad humana de sentirse visto, validado y querido encuentra en estas plataformas un espacio en el que se busca constantemente la aprobación de los demás. Sin embargo, otorgar sentido a la vida a través de la validación externa puede resultar problemático. Estudios han demostrado que los "me gusta" activan el sistema de recompensa del cerebro, estimulando las mismas regiones involucradas en los procesos de adicción. Esto explica por qué el uso de redes sociales puede generar dependencia, al fomentar un ciclo de gratificación instantánea que refuerza la necesidad de aprobación constante.[188]

Es así como el estar conectado, saber que nuestras fotos gustan, o aprobar las fotos de otras personas activan los centros de placer; por esta razón se entiende por qué las personas buscan repetir estas conductas. Los creadores de las redes sociales fomentan esa adicción deliberadamente, como revelan antiguos empleados,[189] pues cuanto más tiempo las personas se encuentren conectadas a la red social, más recaudarán en publicidad, y quienes corren más riesgo son los niños y niñas, quienes a los 11 años más de la mitad ya cuentan con perfiles en las redes sociales.[190]

Los mayores consumidores de redes sociales son los niños, niñas y adolescentes. De acuerdo con el Observatorio Francés de Drogas y Toxicomanía, casi uno de cada dos admite pasar demasiado tiempo en las redes sociales, mientras que el 13% muestra signos de dependencia.[191] Los niños, niñas y adolescentes revisan sus teléfonos hasta 150 veces al día[192] debido a que se aburren rápidamente, esto genera lo que los expertos denominan como “presencia fragmentada”,[193] refiriéndose así a la idea de que las personas pueden tener una presencia en línea a través de múltiples cuentas en diferentes plataformas de

---

[187] DW Documental, “La comercialización de la propia imagen: los peligros de las redes sociales *”, Vídeo de YouTube*, 2022, https://www.youtube.com/watch?v=DWqLAlsiPbE.

[188] Ibíd.

[189] Netflix, “Nada es privado: Documental”.

[190] La comercialización de la propia imagen.

[191] Ibíd.

[192] DW Documental, “Multitasking - ¿Cuánto se puede hacer al mismo tiempo?”, *Vídeo de YouTube*, 2022, https://www.youtube.com/watch?v=qGQwvd6bd1I.

[193] Juan Carlos Andrade Medrano y Patricio Iván Rosas Flores, “Las redes sociales como lugar de construcción de contrapoder”, 2017, 14.

redes sociales, en lugar de tener una única presencia cohesiva en una sola plataforma, así como entre la vida real y la digital; este problema sucede tanto en el trabajo como en el tiempo libre, y muchas personas no son conscientes.

Así, el lapso de atención cambia de generación en generación. Para las nuevas generaciones, debe suceder algo nuevo con más frecuencia, por ejemplo, la atención de la generación Z dura un 25% menos que la de sus antecesores. Los *millenials* pueden mantener la atención durante 12 segundos, mientras que los *centenials* solo durante 8.[194] Los científicos hablan de una creciente y preocupante "ansia de estímulos", una especie de adicción,[195] siendo de esto responsables las células nerviosas del cerebro, denominado "núcleo accumbens";[196] donde se encuentra el sistema de recompensa de nuestro cuerpo. Así es como el centro del placer es estimulado por el neurotransmisor de dopamina generando adicciones, pues si este neurotransmisor se acopla a los receptores correspondientes produce sensaciones positivas que se busca experimentar de manera repetida. Así, si el sistema de recompensa se activa constantemente por una nueva sustancia, se puede desarrollar una especie de adicción.[197]

Estas distracciones influyen en que el centro de placer humano se encuentre en búsqueda constante de nuevos estímulos, para así liberar dopamina, que es la hormona de la felicidad. Esto puede explicarse desde la neurociencia, que indica que el cerebro está sujeto a un proceso de maduración donde el lóbulo frontal tarda un tiempo relativamente largo en madurar hasta un estado adulto, de modo que durante la pubertad esta estructura cerebral aún no es capaz de desarrollar procesos de inhibición correspondiente a los crecientes impulsos emocionales.

Por lo tanto, los niños, niñas y adolescentes son más vulnerables al uso de dispositivos digitales debido a su etapa de desarrollo, su falta de habilidades de

---

[194] Think with Google, "Generación Y (millenials) y Z: características y diferencias", *Think with Google*, accedido 2 de mayo de 2023, párr. 26, https://www.thinkwithgoogle.com/intl/es-es/insights/tendencias-de-consumo/generaciones-y-y-generacion-z-en-que-se-diferencian-y-como-captar-su-atencion.

[195] DW Documental, "Multitasking - ¿Cuánto se puede hacer al mismo tiempo?".

[196] El núcleo accumbens es una estructura ubicada en el cerebro que forma parte del sistema de recompensa y está involucrada en la regulación de la motivación y el placer. Recibe información de diversas áreas del cerebro y está estrechamente relacionado con la liberación de dopamina, un neurotransmisor asociado con la sensación de placer y recompensa. Se sabe que el núcleo accumbens juega un papel importante en la adicción, ya que la activación de esta área del cerebro se asocia con el uso de drogas y comportamientos adictivos. En H.A. Tejeda, T.S. Shippenberg, y R. Henriksson, "The dynorphin/kappa-opioid receptor system and its role in psychiatric disorders", Cellular and Molecular Life Sciences 77, n.º 5 (2020): 857-80.

[197] Ibíd.

autorregulación, la falta de supervisión adecuada y la influencia omnipresente del entorno digital. Los entornos digitales están diseñados para posibilitar esta adicción en las personas, y también ha reducido su tiempo de atención. También es común que los niños, niñas y adolescentes experimenten presión social en línea, como la necesidad de tener muchos seguidores, publicar contenido constantemente para obtener *likes* o ser aceptados por sus pares en línea. Esto puede llevar a la comparación constante y a la baja autoestima.

La niñez y adolescencia son períodos cruciales en el desarrollo cerebral, caracterizado por la plasticidad neuronal y la sensibilidad a estímulos externos. Al ofrecer los entornos digitales una constante gratificación instantánea y una intensa estimulación visual, pueden impactar de manera significativa en la salud mental de los niños, niñas y adolescentes.

### 3.2. Marco de Protección Internacional del Derecho a la Salud Mental de Niños, Niñas y Adolescentes

El Comité de Derechos Económicos, Sociales y Culturales (CDESC), que es un órgano de expertos independientes que monitorea la implementación del PIDESC, en su Observación General N°14 (OG14) proporciona una guía detallada para la interpretación y aplicación del derecho a la salud, definiéndolo como el derecho de toda persona a disfrutar del más alto nivel de salud física y mental posible,[198] lo que incluye acceso a servicios de salud, medicamentos y tecnologías médicas, así como a información y educación sobre la salud. También establece que este derecho abarca los elementos de disponibilidad,[199] accesibilidad,[200] aceptabilidad[201] y calidad,[202] lo que implica el acceso a servicios de salud oportunos, así como a determinantes sociales de la salud, tales como vivienda adecuada, agua potable, saneamiento, alimentos nutritivos y ambiente sano.

Esta Observación General no analiza el derecho a la salud mental bajo un enfoque intergeneracional, pero indica que se deben tomar medidas para prevenir y tratar los

---

[198] Comité de Derechos Económicos, Sociales y Culturales, "Observación General No. 14: El derecho al disfrute del más alto nivel posible de salud", 11 de agosto de 200d. C., 22° período de sesiones, párr. 1.

[199] "Número suficiente de establecimientos, bienes y servicios públicos de salud y centros de atención de la salud, así como de programas", ibíd., párr. 12.

[200] "Accesibles a todos, sin discriminación, a los sectores más vulnerables y marginados de la población, sin discriminación alguna", ibíd.

[201] "Los establecimientos y servicios deben ser respetuosos de la ética médica y culturalmente apropiados", ibíd.

[202] "Apropiados desde el punto de vista científico y médico y ser de buena calidad, lo que requiere personal médico capacitado, medicamentos y equipo hospitalario científicamente aprobados y en buen estado, agua limpia potable y condiciones sanitarias adecuadas". Ibíd.

trastornos mentales en los NNA,[203] así como para promover su bienestar psicológico.[204] También se manifiesta que se deben proporcionar a los adolescentes un entorno seguro, que les permita participar en la toma de decisiones que afecten a su salud mental.[205]

La OG-14 tampoco cuenta con información que vincule el derecho a la salud mental con las nuevas tecnologías (fue publicada en el año 2000), no obstante, establece que los Estados tienen la responsabilidad de garantizar el acceso a servicios de salud mental de calidad y culturalmente adecuados, así como de proteger a las personas de prácticas que puedan afectar negativamente a su salud mental. Lo último mencionado es importante porque lo que se sostiene es que el modelo de negocio de las redes sociales puede crear adicción, lo que conllevaría a la vulneración del derecho a la salud mental de los NNA,[206] además de la vulneración del derecho a la privacidad a través de la falta de protección de datos personales.

Ahora bien, la Relatoría Especial sobre el derecho de toda persona al disfrute del más alto nivel posible de salud física y mental de Naciones Unidas es, sin lugar a duda, la entidad que ha concebido un mayor contenido y alcance al derecho a la salud mental. Así, Entre 2017 y 2020, esta Relatoría publica varios informes sobre salud mental (A/HRC/35/21, A/HRC/41/34 y A/HRC/41/34), concibiéndola como un derecho integral e interdependiente de otros derechos humanos. Esta visión supera la tradicional ausencia de enfermedad para vincularla con condiciones de vida dignas, autonomía personal y participación activa en la vida comunitaria. Todos los informes rechazan los modelos biomédicos coercitivos y defienden la necesidad de servicios de salud mental comunitarios, no discriminatorios y centrados en los derechos humanos.

El informe de 2017 (A/HRC/35/21) sienta las bases de este enfoque al exigir servicios accesibles, aceptables y libres de institucionalización forzada.[207] El de 2019 (A/HRC/41/34) amplía el análisis hacia los determinantes estructurales de la salud

---

[203] Ecuador, *Constitución de la República del Ecuador*, art. 35.

[204] Comité de Derechos Económicos, Sociales y Culturales, "Observación General No. 14: El derecho al disfrute del más alto nivel posible de salud", 11 de agosto de 200d. C., 22° período de sesiones, párr. 22.

[205] Ibíd., párr. 23.

[206] Diana Janely Cárdenas Gutiérrez, "Consecuencias Psicológicas del uso Excesivo de las Redes Sociales en Niños y Jóvenes" (Universidad Católica de Cuenca, 2024), https://dspace.ucacue.edu.ec/bitstreams/083878dc-cf9c-41bd-b7ca-68cf9ccfd21f/download, 16.

[207] Consejo de Derechos Humanos, «Informe del RE sobre el derecho a la salud mental», 28 de marzo de 2017, A/HRC/35/21, párrs. 54-62.

mental, como la educación, la igualdad, la vivienda y la infancia.[208] También menciona que la lista de determinantes básicos de la salud establecidas en la OG14 "no tiene carácter exhaustivo y debe interpretarse a la luz de la evolución de las normas y de los conocimientos científicos";[209] y que "se reconoce cada vez más que el entorno psicosocial es tan importante para la salud como el entorno físico.[210] Finalmente, el informe de 2020 (A/HRC/44/48) introduce amenazas globales emergentes como el cambio climático, la vigilancia digital y las pandemias, señalando la necesidad de respuestas integrales no coercitivas.[211]

En conjunto, los tres informes establecen los componentes esenciales del derecho a la salud mental: servicios de calidad (disponibles, accesibles, aceptables y basados en evidencia científica), atención a los determinantes estructurales y sociales, participación significativa de personas usuarias en la toma de decisiones políticas y terapéuticas, y protección frente a amenazas globales que exacerban las desigualdades.[212] Esta evolución muestra un claro tránsito desde la formulación de marcos normativos hacia una visión holística y preventiva que incorpora la justicia social y ambiental como pilares del derecho a la salud mental.

En 2016, esta Relatoría publicó el informe A/HRC/32/32 sobre el derecho a la salud física y mental de los adolescentes, en el cual lo reconoce como un aspecto esencial de su bienestar integral (abarcando su desarrollo físico, emocional y social) y subraya la necesidad de un enfoque basado en derechos humanos que reconozca la capacidad progresiva de los jóvenes para tomar decisiones autónomas, adoptando así una perspectiva intergeneracional de la salud mental adolescente.[213] En entornos digitales, se subraya que estos espacios ofrecen oportunidades para el acceso a información y redes de apoyo,[214] pero también plantean riesgos como el ciberacoso, la explotación y la violación de la privacidad, que afectan su salud mental.[215] El informe advierte que la rápida

[208] Consejo de Derechos Humanos, "El papel de los determinantes de la salud en el avance del derecho a la salud mental. Informe del Relator Especial sobre el derecho de toda persona al disfrute del más alto nivel posible de salud física y mental", 12 de abril de 2019, A/HRC/41/34, párrs. 11, 63-69.

[209] Ibíd, párr. 16.

[210] Ibíd.

[211] Consejo de Derechos Humanos, «Salud mental y derechos humanos: Establecer una agenda global basada en los derechos. Informe de la Relatora Especial sobre el derecho de toda persona al disfrute del más alto nivel posible de salud física y mental», 15 de abril de 2020, A/HRC/44/48, párrs 71-75.

[212] Ibíd, párrs. 60, 63-67, 71-79

[213] Consejo de Derechos Humanos, "Informe al Consejo de Derechos Humanos (enfoque principal: derecho a la salud de los adolescentes). Informe del Relator Especial sobre el derecho de toda persona al disfrute del más alto nivel posible de salud física y mental", 4 de abril de 2016, A/HRC/32/32, párrs 11, 57.

[214] Ibíd, párr. 21.

[215] Ibíd, párrs 17,45.

evolución digital genera una brecha intergeneracional, limitando la capacidad de padres y cuidadores para guiar a los adolescentes en su uso seguro.[216]

Desde un enfoque diferencial por edad, el documento exige estrategias que equilibren la protección con el respeto a la autonomía en línea. Por ejemplo, se insta a los Estados a fortalecer marcos legales contra el abuso digital,[217] promover educación en seguridad en línea y garantizar servicios de salud mental accesibles y libres de estigma.[218] Además, se critica la patologización de identidades LGBTQ+,[219] exigiendo servicios que respeten la diversidad. El informe integra el principio de evolución de las capacidades,[220] reconociendo que los adolescentes deben participar en decisiones sobre su salud digital, sin restricciones paternalistas injustificadas.

En el informe A/HRC/53/65 de 2023, la Relatora Especial sobre el derecho de toda persona al disfrute del más alto nivel posible de salud física y mental profundiza sobre la salud mental en entornos digitales. El documento analiza de forma crítica cómo la innovación y las tecnologías digitales influyen en la realización efectiva del derecho a la salud, enfocándose particularmente en sus cuatro componentes fundamentales: la disponibilidad, accesibilidad, aceptabilidad y calidad de los establecimientos, bienes y servicios sanitarios.

Así, se menciona que las herramientas digitales pueden ampliar el acceso a la atención médica, especialmente para personas en situación de vulnerabilidad, también se alerta sobre los riesgos asociados, como la extracción masiva de datos personales sin consentimiento, la participación de actores privados con fines de lucro, y las deficiencias en protección de datos, privacidad y rendición de cuentas.[221] En relación con niños, niñas y adolescentes, el informe destaca que si bien las tecnologías digitales pueden brindar oportunidades para mejorar su salud y bienestar, también los exponen a múltiples riesgos, como la explotación sexual en línea, el aislamiento social y los efectos negativos en la salud mental, en especial a raíz de la pandemia de COVID-19.[222]

---

[216] Ibíd., párr. 17.
[217] Ibíd., párr. 45.
[218] Ibíd., párr. 73.
[219] Ibíd.
[220] Ibíd., párr. 57.
[221] Consejo de Derechos Humanos, "Innovación digital, tecnologías y derecho a la salud. Informe de la Relatora Especial sobre el derecho de toda persona al disfrute del más alto nivel posible de salud física y mental", 21 de abril de 2023, A/HRC/53/65, párr. 26 y 59.
[222] Ibíd, párrs. 35 y 42.

Asimismo, se observa con preocupación que la participación de NNA en la gobernanza digital y sanitaria sigue siendo mínima o inexistente.[223] Por ello, la Relatora Especial, junto con la UNESCO, insta a los Estados a investigar y regular los posibles daños de los sistemas digitales e inteligencia artificial en la salud mental, incluyendo fenómenos como el aumento de la ansiedad, la depresión, la adicción o la desinformación.[224] Estos desafíos exigen un enfoque regulatorio basado en derechos humanos, que priorice el interés superior del niño y garantice que el desarrollo tecnológico esté alineado con la promoción de su salud integral.

En la misma línea, el Comité de los Derechos del Niño manifiesta una preocupación creciente por los factores que deterioran la salud mental de niños, niñas y adolescentes. En su Observación General N.º 15, el Comité advierte sobre el aumento de trastornos del desarrollo, depresión, ansiedad, trastornos alimentarios, consumo de sustancias, autolesiones y suicidio en adolescentes, y subraya que uno de los factores emergentes de riesgo es el uso excesivo y adictivo de Internet y otras tecnologías digitales.[225] En consecuencia, hace un llamado a los Estados para que presten mayor atención a los problemas sociales y de comportamiento que debilitan la salud mental y el bienestar psicosocial de este grupo etario.

Complementariamente, en su Observación General N.º 25, el Comité reconoce que los entornos digitales presentan tanto oportunidades como amenazas para los derechos de la infancia. Señala que el desarrollo tecnológico debe estar alineado con el interés superior del niño y que los Estados tienen la obligación de evitar que estos entornos expongan a los NNA a contenidos nocivos o prácticas que comprometan su desarrollo emocional o mental.[226] En particular, alerta sobre la recolección masiva de datos personales de NNA por parte de plataformas digitales, señalando que su tratamiento debe sujetarse a los principios de legalidad, necesidad, proporcionalidad y finalidad específica.[227]Asimismo, prohíbe el uso de estos datos con fines comerciales sin un consentimiento explícito e informado.[228] De forma innovadora, el Comité establece que

---

[223] Ibíd, párr. 35.

[224] Ibíd, párr 28.

[225] Comité de los Derechos del Niño, "Observación General N°15 (2013) sobre el derecho del niño al disfrute del más alto nivel posible de salud (artículo 24)", 17 de abril de 2013, CRC/C/GC/15, Párr 38; Para profundizar sobre los riesgos, ver "Growing up in a digital world: benefits and risks", *The Lancet Child & Adolescent Health*, vol. 2 núm. 2 (febrero de 2018).

[226] Comité de los Derechos del Niño, "Observación general N°25 (2021) relativa a los derechos de los niños en relación con el entorno digital", 2 de marzo de 2021, CRC/C/GC/25, párr. 17.

[227] Ibíd, párrs. 56, 59 y 70.

[228] Ibíd, párrs. 84 y 94.

las tecnologías digitales deben estar sujetas a evaluaciones de impacto en derechos, con especial atención al bienestar psicológico de los NNA, pues prácticas como la publicidad personalizada o el diseño adictivo pueden incidir negativamente en su salud mental.[229] En este marco, el Comité de los Derechos del Niño ha recomendado al Estado ecuatoriano que garantice el acceso efectivo de los niños y adolescentes a servicios de salud mental adecuados y culturalmente pertinentes.[230]

En sus Observaciones Finales al Séptimo Informe Periódico del Ecuador, el Comité retoma los principios de su Observación General N.º 25 y exhorta al país a fortalecer las capacidades institucionales para proteger a la niñez frente a contenidos y productos nocivos en entornos digitales, dotando de recursos suficientes a las entidades competentes.[231] Asimismo, le recomienda reducir las brechas digitales en poblaciones rurales, indígenas, afrodescendientes y montubias, ampliando el acceso equitativo a tecnologías digitales.[232]

Aunque el séptimo informe periódico presentado por el Ecuador ante el Comité de los derechos del Niño expone avances significativos, como el reconocimiento de la salud mental como prioridad estatal y la implementación de programas de prevención del suicidio,[233] aún persisten vacíos relevantes. El documento omite una reflexión crítica sobre los riesgos digitales para la salud mental de los NNA, como la explotación comercial de sus datos personales o la exposición a contenidos nocivos.[234] Tampoco se menciona la aplicación de la Ley Orgánica de Protección de Datos Personales ni se proponen mecanismos que permitan a los NNA ejercer su derecho a la autodeterminación informativa de manera adaptada a su edad. Estas omisiones limitan la comprensión integral del entorno digital como determinante social de la salud mental y evidencian la necesidad de que el Estado incorpore una perspectiva de derechos humanos en sus políticas digitales, centrada en la infancia y en la protección efectiva de su bienestar emocional.

---

[229] Ibíd, párrs. 23 y 38.

[230] Comité de los Derechos del Niño, “Observaciones finales sobre los informes periódicos quinto y sexto combinados del Ecuador”, 26 de octubre de 2017, CRC/C/ECU/CO/5-6, 9.

[231] Comité de los Derechos del Niño, "Observaciones finales sobre el séptimo informe periódico del Ecuador", 27 de febrero de 2025, CRC/C/ECU/CO/7, párr. 24.

[232] Ibíd.

[233] Comité de los Derechos del Niño, "Séptimo informe periódico que el Ecuador debía presentar en 2023 en virtud del artículo 44 de la Convención", 13 de febrero de 2024, CRC/C/ECU/7, párr. 114.

[234] En los párrafos 79, 80 y 81 del informe se establece lo que ha realizado el Ecuador para que los NNA tengan acceso a información apropiada. En Ibíd, párrs. 79-81.

En conclusión, el análisis de los principales instrumentos internacionales muestra un avance significativo en la comprensión del derecho a la salud mental, especialmente en relación con niños, niñas y adolescentes en el entorno digital. Si bien documentos como la Observación General N°14 del Comité DESC sentaron bases importantes, informes más recientes de la Relatoría Especial sobre el derecho a la salud y del Comité de los Derechos del Niño han incorporado nuevas preocupaciones, como el impacto de las tecnologías digitales en el bienestar psicológico de los NNA. Estas tendencias reflejan un cambio hacia una visión holística y preventiva, que reconoce no solo los servicios de salud mental tradicionales, sino también los riesgos estructurales y emergentes que afectan la autonomía, la privacidad y la integridad emocional de la infancia en el entorno digital. A pesar de estos avances, el Ecuador tiene el desafío de adaptar integralmente sus políticas públicas a estos nuevos estándares para garantizar una protección efectiva y adecuada a las realidades actuales.

### 3.3. Marco de Protección Nacional del Derecho a la Salud Mental de Niños, Niñas y Adolescentes

Ahora bien, en enero de 2024 entró en vigencia en el Ecuador la Ley Orgánica de Salud Mental (LOSM), que tiene entre sus fines "reconocer a la salud mental como parte de la atención integral de salud e impulsar la consolidación de una política nacional en salud mental, a fin de que el Estado priorice las acciones en esta materia".[235] De acuerdo con el artículo 17, la Autoridad Sanitaria Nacional tendrá la competencia de emitir, evaluar y controlar la política pública de salud mental. También se crea una red de servicios de salud mental, integrada por la red pública y otros organismos privados o comunitarios que brinden servicios de salud mental. Esta red se organiza bajo la rectoría y liderazgo de la Autoridad Sanitaria Nacional.[236]

Con respecto a las niñas, niños y adolescentes, la norma señala que las instituciones del Sistema Nacional de Salud deberán implementar servicios especializados de salud mental para NNA,[237] y de acuerdo con la disposición transitoria primera, el presidente emitió el 23 de noviembre de 2024, mediante Decreto Ejecutivo 465, el Reglamento General a la Ley Orgánica de Salud Mental. Este Reglamento

[235] Ecuador, *Ley Orgánica de Salud Mental*, Registro Oficial 471, Suplemento, 5 de enero de 2024, art.3 lit.a.

[236] Ibíd., art. 20.

[237] Ibíd., art.8.

establece las directrices para la aplicación de la Ley Orgánica de Salud Mental desde un enfoque comunitario,[238] y reconoce la necesidad de ampliar la oferta de atención en salud mental para niños, niñas y adolescentes con personal capacitado para atender a esta población.[239] Asimismo, establece que toda intervención deberá contar con consentimiento informado de sus representantes legales y garantizar la comprensión y participación activa de los NNA en su proceso terapéutico. De manera positiva, el reglamento enfatiza la necesidad de evitar la sobremedicación e institucionalización, y promueve la intervención temprana y el cuidado de la salud mental desde la etapa perinatal.[240]

Es importante destacar que este reglamento en su artículo 12 reconoce el deber del Estado de priorizar la salud mental sobre intereses comerciales, y que se debe "proteger las políticas de salud mental de la interferencia directa e indirecta de las industrias que puedan tener conflictos de interés",[241] lo cual representa un avance importante en términos de soberanía en políticas públicas y se puede aplicar a la presente situación. Sin embargo, el reglamento no se pronuncia de forma directa sobre los riesgos psicosociales asociados al uso de tecnologías digitales, redes sociales y plataformas en línea por parte de niños, niñas y adolescentes. Esta omisión resulta preocupante frente a la creciente evidencia internacional que advierte sobre los impactos negativos del entorno digital en la salud mental de niños, niñas y adolescentes.

Si bien la Ley Orgánica de Salud Mental representa un avance en el reconocimiento de este derecho en Ecuador, aún carece de una perspectiva actualizada y preventiva que considere las transformaciones digitales del entorno y los nuevos desafíos que estas implican para el bienestar emocional de este grupo de la población. Pese a su poco tiempo en vigencia, ha recibido críticas importantes respecto a su contenido y aplicación. Entre las principales observaciones está su enfoque excesivamente biomédico, que reduce la salud mental a la existencia de "trastornos mentales", sin incorporar adecuadamente conceptos psicológicos como psicodiagnóstico, psicoterapia o el reconocimiento del sufrimiento humano fuera de una lógica patologizante.[242] Esta visión

---

[238] Ecuador, "Reglamento General a la Ley Orgánica de Salud Mental", Decreto Ejecutivo No. 465 § (2024), Registro Oficial Suplemento 697, art. 2.

[239] Ibíd, art. 4.

[240] Ibíd, art. 5.

[241] Ibíd, art. 12.

[242] Verónica Egas, Lenín Jácome Chávez, y Luis Iriarte, "¿Por qué no funciona la Ley de Salud Mental?" (Conversatorio de Salud Mental, Quito-Ecuador, 10 de abril de 2025), https://www.instagram.com/reel/DIjRukGuX9o/?igsh=MXQ0cDltNmRodHhzOQ%3D%3D.

limita la comprensión integral de la salud mental y puede conducir a la medicalización innecesaria del malestar emocional.

Esta crítica al modelo biomédico no es aislada: los informes temáticos de la Relatoría Especial sobre el derecho a la salud de Naciones Unidas (A/HRC/35/21, A/HRC/41/34, A/HRC/32/32) han enfatizado la necesidad de superar visiones reduccionistas que medicalizan o patologizan el malestar social. La Relatoría ha señalado que los enfoques biomédicos coercitivos ignoran los determinantes psicosociales y estructurales de la salud mental, particularmente en niños, niñas y adolescentes, perpetuando prácticas que marginan, estigmatizan y excluyen.[243] En cambio, aboga por servicios basados en derechos humanos, participación activa de los propios adolescentes, enfoques comunitarios y estrategias de prevención que reconozcan su capacidad progresiva de autonomía,[244] especialmente en contextos como los entornos digitales, donde los adolescentes enfrentan nuevos desafíos para su bienestar emocional.

Además, la ley omite la especificidad de las diferentes ramas de la psicología, permitiendo que profesionales de áreas no clínicas puedan intervenir en procesos de atención terapéutica. También se cuestiona que excluye numerosos diagnósticos de su definición de problema de salud pública, despriorizando situaciones que, aunque no clasificadas como trastornos graves, afectan el bienestar emocional de las personas.[245] Estas falencias son particularmente preocupantes en relación con los adolescentes en entornos digitales, quienes enfrentan nuevos riesgos psicosociales (como el ciberacoso, la explotación de datos personales y la adicción tecnológica) que requieren un enfoque más dinámico y preventivo.

Aparte de la LOSM, el Ecuador ha desarrollado un marco normativo importante en materia de niñez, adolescencia y prevención de la violencia vinculada a la salud mental. En el séptimo informe periódico (CRC/C/ECU/7) el Estado detalla una serie de instrumentos normativos dirigidos a reforzar la protección integral de la niñez y adolescencia y a prevenir la violencia vinculada a la salud mental de niñas, niños y adolescentes. Destaca el proyecto de Código Orgánico para la Protección Integral de Niños, Niñas y Adolescentes (COPPINA), que incluye doctrina de protección contra el

[243] Consejo de Derechos Humanos, "Informe al Consejo de Derechos Humanos (enfoque principal: derecho a la salud de los adolescentes). Informe del Relator Especial sobre el derecho de toda persona al disfrute del más alto nivel posible de salud física y mental", párr. 15.

[244] Consejo de Derechos Humanos, "El papel de los determinantes de la salud en el avance del derecho a la salud mental. Informe del Relator Especial sobre el derecho de toda persona al disfrute del más alto nivel posible de salud física y mental", párr. 28.

[245] Ibíd.

maltrato físico y psicológico y establece sanciones educativas, familiares y privadas tras un amplio proceso de consulta con NNA.[246] La Fiscalía General del Estado emitió varias políticas, como "Lineamientos de Política de Prevención del Fenómeno Delictual de Violencia Sexual en contra de NNA" (2020) y, en 2023, la "Política Criminal de Prevención de la Violencia de Género – Lineamientos de Actuación" para abordar denuncias de cualquier tipo de violencia, incluida la psicológica.[247] Asimismo, a través del Sistema de Protección a Víctimas y Testigos (SPAVT) y otros mecanismos, se proporcionan primeros auxilios psicológicos e intervención en crisis a las víctimas, complementados con insumos de protección,[248] y el Ministerio de Educación diseñó 22 herramientas, entre ellas guías para docentes de apoyo psicológico y emocional en situaciones de crisis.[249]

Para la prevención de riesgos psicosociales en el entorno escolar y familiar, el informe menciona la aplicación del Plan Nacional de Prevención de la Violencia Contra la Niñez y Adolescencia y Promoción de Parentalidades Positivas (2018) junto con la Política Nacional de Convivencia Escolar (2021),[250] que impulsa ambientes de paz y prevención de riesgos psicosociales en comunidades educativas.[251] En el ámbito digital, el Consejo de Regulación y Desarrollo de la Información y Comunicación (CORDICOM) adoptó medidas de educación transmedia y capacitación para proteger la integridad psicológica y emocional de NNA frente a contenidos nocivos en línea,[252] y en 2020 se publicó la Política Pública de Internet Seguro para Niñas, Niños y Adolescentes, con el fin de proteger su dignidad e integridad física, psicológica y emocional en el entorno digital.[253]

Pese a las medidas adoptadas por el Ecuador para garantizar el derecho a la salud mental en NNA, es urgente adoptar pasos concretos para acelerar la aprobación del nuevo

---

[246] Comité de los Derechos del Niño, "Séptimo informe periódico que el Ecuador debía presentar en 2023 en virtud del artículo 44 de la Convención", párrs. 20 y 82.

[247] Ibíd, párr. 3; Fiscalía General del Estado, "Políticas y Directrices Institucionales", accedido 27 de abril de 2025, https://www.fiscalia.gob.ec/politicas-y-directrices-institucionales/.

[248] Ibíd, párr. 10.

[249] Ibíd, párr. 14.

[250] Ministerio de Educación Ecuador, "Política Nacional de Convivencia Escolar", 12 de marzo de 2021, https://educacion.gob.ec/wp-content/uploads/downloads/2021/04/Politica-Nacional-de-Convivencia-Escolar.pdf.

[251] Ibíd, párr. 83.

[252] Ibíd, párr. 80.

[253] Ibíd, párr. 81; La DINARP trabajó en la construcción y publicación de la página https://internetsegura.gob.ec/ que contiene videos, reportajes, juegos, ideas y contenido especializado para niñas, niños, adolescentes, familias y docentes. Este espacio informativo ofrece herramientas lúdicas acerca de las oportunidades y riesgos de la red y cómo actuar ante alertas.

Código de Niñez y Adolescencia,[254] aprobar un plan nacional de protección con recursos suficientes;[255] establecer un organismo interministerial de alto nivel para coordinar la aplicación de la Convención;[256] y reforzar la asignación de recursos y la recopilación de datos desagregados por edad, sexo, etnia y situación de vulnerabilidad.[257] Al mismo tiempo, es preocupante la falta de aplicación efectiva de los planes y políticas de prevención de la violencia en barrios, escuelas y hogares.[258]

Respecto al entorno digital, es imperativo adoptar medidas legislativas que permitan a las autoridades proteger a los NNA de la violencia y de la información y productos nocivos en línea, facultándolas para adoptar medidas sin autorización judicial previa,[259] por ejemplo, así como impulsar programas de inclusión digital, especialmente en zonas rurales e indígenas, y esfuerzos de alfabetización digital para reducir las brechas y salvaguardar la salud mental de NNA en los espacios virtuales.[260]

De todo lo manifestado se puede señalar que, aunque el Ecuador ha dado pasos importantes con la aprobación de la Ley Orgánica de Salud Mental y el desarrollo de su reglamento, así como de políticas y planes nacionales orientados a la protección de niñas, niños y adolescentes, persisten limitaciones estructurales que deben ser superadas. La falta de un enfoque integral que trascienda el modelo biomédico, así como la omisión de los riesgos que plantea el entorno digital para la salud mental de los adolescentes, revelan vacíos críticos en la normativa y su aplicación. Frente a los desafíos contemporáneos, especialmente en los entornos digitales, resulta urgente actualizar las políticas públicas, fortalecer la protección de datos personales, y diseñar intervenciones que reconozcan la autonomía progresiva de los adolescentes, su derecho a entornos digitales seguros y su participación activa en las decisiones que afectan su bienestar emocional.

## 4. Desafíos en la protección de la salud mental y los datos personales de Niños, Niñas y Adolescentes

El derecho a la protección de datos personales es un derecho humano estrechamente vinculado con la privacidad y la salud mental en entornos digitales. En este

[254] Comité de los Derechos del Niño, "Observaciones finales sobre el séptimo informe periódico del Ecuador", párr. 6.
[255] Ibíd, párr. 7.
[256] Ibíd, párr. 8.
[257] Ibíd, párrs. 9 y 10.
[258] Ibíd, párr. 25.
[259] Ibíd, párr. 24 a) y b).
[260] Ibíd, párr. 24 b).

contexto, el modelo de negocio adoptado por muchas plataformas en Internet, basado en la recolección masiva y el uso intensivo de datos personales, puede generar impactos negativos en la salud mental de niños, niñas y adolescentes.[261] Estos modelos operan maximizando el tiempo de permanencia del usuario en la plataforma para incrementar sus ingresos a través de publicidad dirigida. Sin embargo, este objetivo se logra con frecuencia mediante mecanismos de manipulación algorítmica, como la radicalización del pensamiento,[262] la exposición reiterada a contenidos polarizantes y la difusión de noticias falsas.[263] Tales prácticas pueden afectar de manera significativa el bienestar psicológico de los NNA, al incidir en su percepción del mundo, en su autoestima[264] y en su equilibrio emocional.[265] En este sentido, la venta o cesión de datos personales por parte de las grandes corporaciones tecnológicas no solo representa una posible violación a los derechos a la privacidad y a la protección de datos personales, sino que también plantea riesgos concretos para la salud mental, al exponer a los usuarios, especialmente a los más jóvenes, a dinámicas digitales que los sobre estimulan, los aíslan o los vulneran emocionalmente.[266]

Se presentan casos documentados que evidencian el impacto psicológico negativo de las tecnologías digitales en niños, niñas y adolescentes. Por ejemplo, durante una audiencia en el Senado de Estados Unidos, el director ejecutivo de *Meta*, Mark Zuckerberg, se disculpó públicamente ante las familias cuyos hijos han sufrido daños por el uso de redes sociales como *Instagram* y *Facebook*. Dirigiéndose a ellas, expresó: “Lamento todo lo que han pasado, es terrible. Nadie debería tener que pasar por las cosas

---

[261] Rodrigo Jácob Moreira de Freitas et al., “Percepciones de los adolescentes sobre el uso de las redes sociales y su influencia en la salud mental”, *Enfermería Global* 20, nº 64 (2021): 324-64, doi:10.6018/eglobal.462631, 332.

[262] Las redes sociales son un espacio en el que los usuarios comparten información personal y opiniones públicamente. Esta información es recopilada y utilizada por los algoritmos de las redes sociales para mostrarnos contenido relevante y personalizado, lo que puede resultar enuna burbuja informativa que nos aísla de opiniones diferentes a las nuestras. En Brian Martin Ríos Nicoli, “Radicalización digital: el efecto de las redes sociales en el extremismo político y el discurso del odio”, *Ciencia Latina Revista Científica Multidisciplinar* 7, n.º 1 (23 de marzo de 2023): 10749-55, doi:10.37811/cl_rcm.v7i1.5247, 6.

[263] https://plus.google.com/+UNESCO, “Crecer En La Era de Las Fake News”, *UNESCO*, 6 de abril de 2021, párr. 10, https://es.unesco.org/courier/2021-2/crecer-era-fake-news.

[264] Helen Thai et al., "Reducing Social Media Use Improves Appearance and Weight Esteem in Youth with Emotional Distress.", *Psychology of Popular Media* 13, n.º 1 (enero de 2024): 162-69, doi:10.1037/ppm0000460, 167.

[265] Yalda T. Uhls et al., "Five days at outdoor education camp without screens improves preteen skills with nonverbal emotion cues", *Computers in Human Behavior* 39 (1 de octubre de 2014): 387-92, doi:10.1016/j.chb.2014.05.036, 389.

[266] Karen Frankel Heffler et al., “Early-Life Digital Media Experiences and Development of Atypical Sensory Processing”, *JAMA Pediatrics* 178, n.º 3 (1 de marzo de 2024): 266, doi:10.1001/jamapediatrics.2023.5923, E2.

que han sufrido sus familias".[267] La audiencia, centrada en la protección de los niños en entornos digitales, abordó temas como el ciberacoso, la salud mental y la exposición a contenidos perjudiciales, mientras los legisladores cuestionaban duramente a los líderes de las principales plataformas sobre su responsabilidad y medidas preventivas. Evan Spiegel, CEO de *Snap*, también ha ofrecido disculpas a las familias de jóvenes que fallecieron tras adquirir drogas a través de *Snapchat*, reconociendo la necesidad de mejorar las medidas de seguridad en sus plataformas.[268]

Así, la situación actual del Ecuador frente a los nuevos desafíos que plantea la protección de datos personales y su impacto en la salud mental de niños, niñas y adolescentes en entornos digitales evidencia avances importantes,[269] pero también revela profundas limitaciones estructurales. A nivel normativo, se reconoce como un paso positivo la aprobación de la Ley Orgánica de Protección de Datos Personales y la Ley Orgánica de Salud Mental, que reflejan una creciente sensibilidad hacia estos derechos. Sin embargo, estos instrumentos aún carecen de una articulación efectiva que permita abordar de manera integral la relación entre salud mental y explotación de datos en el entorno digital.

Mientras los estándares internacionales han evolucionado hacia enfoques holísticos que consideran la salud mental desde una perspectiva interseccional, estructural y preventiva (particularmente frente a fenómenos como la manipulación algorítmica y la comercialización de datos personales), el marco nacional ecuatoriano todavía permanece anclado a lógicas fragmentadas y reactivas.[270]

---

[267] BBC News Mundo, "Zuckerberg: el jefe de Facebook se disculpa ante las familias de los niños que han sufrido daños por culpa de las redes sociales", *BBC News Mundo*, 1 de febrero de 2024, https://www.bbc.com/mundo/articles/c72gze8r05jo, párr. 7.

[268] Clare Duffy Fung Brian, "Mark Zuckerberg se disculpa con familias por los daños causados en redes sociales", *CNN*, 31 de enero de 2024, https://cnnespanol.cnn.com/2024/01/31/mark-zuckerberg-se-disculpa-familias-danos-causados-redes-sociales-trax, párr. 18.

[269] El Estado ha suscrito y asimilado los principios del Reglamento General de Protección de Datos de la UE (con su énfasis en responsabilidad proactiva, evaluaciones de impacto y controles transfronterizos) y algunos estándares elaborados por la Relatoría Especial de la ONU sobre salud física y mental (A/HRC/35/21; A/HRC/41/34; A/HRC/44/48).

[270] Aunque la LOSM y su reglamento (Decreto 465-2024) incorporan disposiciones sobre consentimiento informado, servicios comunitarios y vetan las industrias con conflictos de interés, no contemplan explícitamente los riesgos derivados de la extracción y el perfilado masivo de datos de NNA. Por su parte, la LOPDP establece un régimen de consentimiento y DPIA (evaluaciones de impacto), pero no exige que estas evaluaciones incluyan criterios de salud mental infantil ni que los operadores adapten sus algoritmos a los niveles de vulnerabilidad psicosocial de los menores. A ello se suman lagunas en las políticas transversales (Internet Seguro para NNA, CORDICOM, planes de convivencia escolar) que carecen de mandatos vinculantes para las plataformas digitales, y la ausencia de un ente interministerial que coordine salud, educación y protección de datos bajo el principio del interés superior del niño.

Esta desconexión normativa deja a los niños, niñas y adolescentes en una situación de alta vulnerabilidad ante los riesgos que plantea el ecosistema digital actual. La opacidad de los algoritmos, la ausencia de controles sobre la recolección masiva de datos personales, y la falta de participación significativa de la niñez y adolescencia en los procesos de gobernanza digital son problemas que, pese a su gravedad, no han sido enfrentados de manera decidida en las leyes nacionales. Tampoco se ha incorporado plenamente el principio de autonomía progresiva en la protección de datos personales, ni se han desarrollado mecanismos específicos que garanticen el derecho a la salud mental en entornos virtuales, lo que perpetúa un enfoque adultocéntrico que no reconoce la agencia de los NNA en el mundo digital.

Ante este panorama, resulta indispensable replantear los marcos legales y las políticas públicas desde una perspectiva de derechos humanos que priorice el interés superior del niño y la prevención de daños psicosociales. Sería deseable fortalecer la Ley de Protección de Datos Personales incorporando disposiciones específicas sobre la protección reforzada de los datos de niños, niñas y adolescentes, incluyendo la obligación de realizar evaluaciones de impacto de los tratamientos de datos desde un enfoque de salud mental.[271] Asimismo, el reconocimiento explícito del derecho a entornos digitales seguros y respetuosos del bienestar emocional infantil y adolescente debería ser parte del sistema nacional de protección de datos. No se trata solo de proteger la privacidad, sino de garantizar espacios que promuevan la autonomía, el bienestar psicológico y el desarrollo sano en el entorno digital, en consonancia con las tendencias más avanzadas en el derecho internacional.

[271] Por ejemplo, se podría establecer la obligación de realizar evaluaciones de impacto en los sitios web donde se valore el riesgo de adicción, ciberacoso y exposición a contenidos nocivos, y se diseñen medidas preventivas (como disponer límites de tiempo de pantalla o ecosistemas digitales saludables).

# Capítulo segundo
# Impactos del entorno digital en el derecho a la salud mental de niños, niñas y adolescentes

La privacidad no es una opción,
y no debería ser el precio que aceptamos por
simplemente estar en Internet
(Gary Kovacs 2011)

En este capítulo se analiza la evolución del acceso a Internet en Ecuador, evidenciando un crecimiento notable en la conectividad, especialmente tras la pandemia del COVID-19. Se presentan datos que muestran cómo la penetración de Internet en hogares y el uso de dispositivos digitales han aumentado significativamente, alcanzando a un mayor porcentaje de niños, niñas y adolescentes. Sin embargo, esta expansión digital no ha sido equitativa, ya que se observan brechas territoriales y socioeconómicas que afectan la calidad del acceso. Este fenómeno ha empeorado ciertos problemas de salud mental, al exponer a NNA a riesgos como la sexualización temprana, ansiedad, depresión, violencia digital y comportamientos de hiperconsumo, alimentados por la constante interacción en el entorno digital.

Por otro lado, el capítulo adopta un enfoque cualitativo a través de entrevistas con profesionales de la psicología y expertos en protección de datos, que permiten comprender de forma integral cómo el entorno digital impacta la salud mental de la población infantil y adolescente. Se destaca la importancia de la corresponsabilidad entre familias, el Estado y las empresas tecnológicas para establecer medidas preventivas y regulaciones efectivas que salvaguarden el derecho a la salud mental y la privacidad. Además, se exploran propuestas alternativas basadas en la cooperación internacional y en un enfoque holístico que combine la normativa con políticas públicas, educación y estrategias de protección para mitigar los riesgos emergentes en el entorno digital.

## 1. Panorama de la Conectividad Digital en la Infancia y Adolescencia Ecuatoriana

El acceso a Internet aumentó significativamente desde la pandemia del COVID-19. El Instituto Nacional de Estadísticas y Censos (INEC) publicó los datos sobre tecnologías de la información y comunicación del año 2019, donde a través de encuestas establece que en ese año solo el 45,5 % de hogares a escala nacional contaban con acceso

a Internet;[272] en otras palabras, más de la mitad de las familias no contaban con este servicio en su casa.

Sin embargo, en el año 2020 el acceso a Internet aumenta en 11,5 puntos porcentuales con respecto a 2019, así como el porcentaje de personas que lo utilizan en sus celulares.[273] Esto tiene una estrecha relación con la vigencia de las clases virtuales, así como del teletrabajo debido a la pandemia. Asimismo, el INEC muestra que en 2020 el 44,6 % de la población ecuatoriana de más de 5 años utilizaba ya redes sociales.[274]

El 2024 es un año de disrupción digital, con niveles cada vez más altos de acceso a Internet. De acuerdo con *Datareportal,*[275] entre 2023 a 2024 han aumentado las usuarias y usuarios de Internet en el Ecuador en 571 mil (3,9 %), llegando así al 83,6 % la tasa de penetración de Internet. Así, en el Ecuador utilizan Internet 15.29 millones de personas, de las 18.28 millones[276] que habitan en el país.[277] Esto demuestra una clara tendencia de aumento en el acceso a Internet en la población.

Esta tendencia también se corrobora por el INEC, que demuestra cómo ha aumentado en el país el acceso a Internet y su uso de julio de 2022 (60,4 %) a julio de 2023 (62,2 %):

---

[272] Ecuador, Instituto Nacional de Estadística y Censos, "Tecnologías de la Información y Comunicación-TIC", *Instituto Nacional de Estadística y Censos*, accedido 18 de diciembre de 2020, párr. 2, https://www.ecuadorencifras.gob.ec/tecnologias-de-la-informacion-y-comunicacion-tic/.

[273] Instituto Nacional de Estadística y Censos, "Tecnologías de la Información y Comunicación-TIC".

[274] Instituto Nacional de Estadística y Censos, "Tecnologías de la Información y Comunicación 2020", abril de 2021, https://www.ecuadorencifras.gob.ec/documentos/web-inec/Estadisticas_Sociales/TIC/2020/202012_Principales_resultados_Multiproposito_TIC.pdf, 23.

[275] DataReportal es una Plataforma que ofrece información global sobre tendencias digitales. Proporciona informes gratuitos que ayudan a comprender lo que las personas realmente hacen en línea. Ver: https://datareportal.com/

[276] De acuerdo con el último censo del Ecuador (2022), en el país residen 16.938.986 personas. Instituto Nacional de Estadística y Censos, "Censo Ecuador 2022", *Censo Ecuador*, 2023, 1, https://www.censoecuador.gob.ec/.

[277] DataReportal, "Digital 2024: Ecuador", *DataReportal*, 23 de febrero de 2024, 6, https://datareportal.com/reports/digital-2024-ecuador.

Tabla 1
**Hogares y personas con acceso a Internet**

| Indicadores de TIC 2023* (Nacional) | jul-22 | jul-23 |
|---|---|---|
| Hogares con Acceso a internet (%) | 60,4 | 62,2 |
| Personas que utilizan internet[1] (%) | 69,7 | 72,7 |
| Personas que tienen celular activado (%) | 58,8 | 59,6 |
| Personas que tienen teléfono inteligente[2] (%) | 52,2 | 55,6 |
| Analfabetismo digital [3] (%) | 8,2 | 7,6 |

Notas:
1. Personas que utilizan internet, se refiere a la población de 5 y más años que ha usado internet en los últimos 12 meses, desde cualquier lugar.
2. Porcentaje de teléfono inteligente.- se refiere a la población de 5 y más años con celular activado smartphone con respecto a la población de 5 y más años.
3. Se considera Analfabeta Digital a una persona de 15 a 49 años cuando cumple simultáneamente tres características: 1) No tiene celular activado 2) En los últimos 12 meses no ha utilizado computadora 3) En los últimos 12 meses no ha utilizado internet.
*La información del 2022 corresponde a la Encuesta de Empleo, Desempleo y Subempleo – Enemdu.

Fuente y elaboración: INEC (2022)

Si bien existen diferencias entre los resultados del INEC con *Datareportal*, sobre el acceso al internet en el Ecuador, en ambos se demuestra cómo aumenta el acceso a Internet con el paso de los años.

También ha aumentado el porcentaje de niños, niñas y adolescentes que cuentan con acceso a Internet y redes sociales en el Ecuador. Se realizó una solicitud de información al INEC en noviembre de 2023, entidad que puso en conocimiento la Encuesta Nacional de Empleo, Desempleo y Subempleo (ENEMDU), que aunque tiene como objetivo conocer la actividad económica y las fuentes de ingresos de la población, también cuenta con información sobre acceso a Internet de este grupo de la población.

Así, con corte a julio de 2023, el 64,4 % de niños, niñas y adolescentes de 5 a 17 años tiene acceso a Internet en sus hogares, aumentando en casi 20 puntos en comparación con el año 2019:

Tabla 2
**Porcentaje de niños, niñas y adolescentes de 5 a 17 años con acceso a Internet en sus hogares en el año 2023**

| Desagregación | Nacional |
|---|---|
| NNA con acceso a Internet en sus hogares | 64,4 % |

Fuente: Encuesta Nacional de Empleo, Desempleo y Subempleo, Instituto Nacional de Estadísticas y Censos
Elaboración: Propia

Mientras que el porcentaje de personas de esta misma edad que utilizan Internet aumenta a 69,7%:

Tabla 3
**Porcentaje de niños, niñas y adolescentes de 5 a 17 años que utilizan Internet en el año 2023**

| Desagregación | Nacional |
|---|---|
| Personas que utilizan Internet | 69,7 % |

Fuente: Encuesta Nacional de Empleo, Desempleo y Subempleo, Instituto Nacional de Estadísticas y Censos
Elaboración: Propia

Estas cifras demuestran que, por cada 10 niños, niñas y adolescentes, al menos 7 tienen acceso a Internet. Es claro que la tendencia indica el aumento gradual de acceso a Internet para todas las personas, incluyendo a niños, niñas y adolescentes.

El 44,1 % de niños, niñas y adolescentes de 5 a 17 años utiliza Internet para comunicaciones y redes sociales, el 23,1 % para educación y aprendizaje, el 30,1 % para actividades de entretenimiento, el 2,2 % para obtener información y el 0,5 % para otros fines:[278]

Como se puede observar, en el mundo contemporáneo, el uso de la tecnología ha permeado profundamente la vida de niños, niñas y adolescentes ecuatorianos. Sin embargo, esta interacción no es uniforme ni sus efectos son iguales para todos los grupos. De acuerdo con ONU Mujeres, la violencia hacia las mujeres y niñas se ha facilitado por la tecnología. Una de cada diez mujeres en la Unión Europea ha sufrido ciberacoso desde los 15 años;[279] el 60 % de las usuarias de Internet en los Estados Árabes ha estado expuesta a violencia en línea en el último año;[280] el 49 % de las mujeres de Uganda informó haber sido hostigada en línea;[281] el 85 % de las mujeres de Corea del Sur

[278] La categoría "Otros" corresponde a comprar u ordenar productos o servicios (delivery, comercio electrónico), Almacenamiento en Internet para guardar documentos, trámites con organismos gubernamentales en línea, leer, descargar libros electrónicos, periódicos, etc.; para vender bienes o servicios (comercio electrónico), banca electrónica y otros servicios financieros, por salud (agendar citas médicas). En INEC, Encuesta Nacional de Empleo, Desempleo y Subempleo, Instituto Nacional de Estadísticas y Censos.

[279] ONU Mujeres, "Hechos y cifras: Poner fin a la violencia contra las mujeres", ONU Mujeres, accedido 23 de julio de 2024, https://www.unwomen.org/es/what-we-do/ending-violence-against-women/facts-and-figures, 3.

[280] Ibíd., 4.

[281] Ibíd., 5.

experimentaron incitación al odio en línea,[282] y el 73 % de las periodistas ha experimentado violencia en línea.[283]

En suma, el acceso a Internet entre niños, niñas y adolescentes en el Ecuador ha experimentado un crecimiento sostenido en los últimos años, impulsado principalmente por la pandemia y la creciente digitalización de la vida cotidiana. Este fenómeno, aunque ofrece oportunidades para el aprendizaje, la comunicación y el entretenimiento, también plantea desafíos importantes en términos de bienestar psicosocial, exposición a contenidos nocivos y riesgos de violencia en línea. La tendencia ascendente en el uso de redes sociales por parte de esta población exige una reflexión profunda sobre las políticas públicas, la regulación digital y las estrategias de protección, para garantizar que el entorno digital sea seguro, inclusivo y respetuoso de los derechos de niñas, niños y adolescentes.

## 2. Presentación del estudio y resultados

La presente investigación adopta un enfoque cualitativo de carácter exploratorio y crítico de derechos humanos, cuyo propósito es comprender en profundidad la relación entre el entorno digital y el derecho a la salud mental de niños, niñas y adolescentes en Ecuador. Este paradigma metodológico privilegia el análisis de experiencias, percepciones y significados en contextos reales, sin reducir los fenómenos a indicadores cuantitativos, sino situándolos en su complejidad sociocultural y normativa.

Para recolectar la información, se combinaron entrevistas semiestructuradas y análisis documental y normativo. Las entrevistas personales, guiadas por una pauta de preguntas abiertas,[284] permitieron explorar de manera flexible las visiones de nueve informantes clave: cuatro psicólogos, cuatro expertos en protección de datos y una usuaria de la plataforma *Worldcoin*.[285] Este diálogo directo enriqueció el estudio con narrativas vivas sobre salud mental en el entorno digital. Paralelamente, el análisis de documentos (desde la Constitución y la Ley Orgánica de Protección de Datos Personales hasta sentencias de la Corte Interamericana, observaciones al Ecuador de relatorías de la ONU y artículo académicos) aportó el contexto legal, institucional y conceptual necesario para contrastar las opiniones expertas con la realidad normativa y detectar vacíos o tensiones.

---

[282] Ibíd., 6.
[283] Ibíd., 37.
[284] Ver Anexo 3.
[285] Caso abordado en el tercer capítulo para realizar litigio estratégico.

Los criterios de inclusión de las personas entrevistadas se basaron en diversidad de género, en su experiencia profesional o vivencial en salud mental infantil/adolescente o en protección de datos de NNA, así como en su disponibilidad para participar entre mayo y junio de 2024.[286] Todos otorgaron consentimiento informado previo, y se garantizó el anonimato mediante seudónimos para las víctimas.[287] Este muestreo intencional busca asegurar que las voces representen tanto el ámbito clínico y educativo como el jurídico y tecnológico, cubriendo así la pluralidad de perspectivas necesarias para abordar un tema multidimensional.

El análisis se estructuró en cinco categorías de estudio, cada una con sus subcategorías y definición operativa:

Tabla 4
**Categorías de estudio, subcategorías y Definición operativa**

| Categoría | Subcategorías | Definición operativa |
|---|---|---|
| Impacto en la salud mental | Sexualización, ansiedad, depresión, hiperconsumo, violencia digital, hiperconectividad | Agrupa los efectos psicoemocionales derivados del uso de entornos digitales por parte de niños, niñas y adolescentes. |
| Pandemia y virtualidad | Educación, salud emocional, brecha digital | Valora los cambios estructurales en el entorno digital de los NNA durante el confinamiento por COVID-19. |
| Corresponsabilidad | Rol de la familia, rol del Estado, rol de las empresas de datos | Examina la distribución de responsabilidades entre actores clave para proteger los derechos de NNA en entornos digitales. |
| Protección de datos personales | Riesgos en redes, marco legal, instituciones de supervisión | Centra su atención en la seguridad de la identidad digital de los NNA y el cumplimiento del marco jurídico. |
| Alternativas | Cooperación internacional, enfoque integral | Incluye propuestas de solución multidimensionales para fortalecer la protección de los derechos de los NNA. |

Fuente: Anexo 4.
Elaboración propia, 2025

El análisis de datos cualitativos siguió un proceso de varias etapas: primero, la transcripción literal de cada entrevista; luego, la codificación abierta para identificar fragmentos significativos ligados a las categorías; a continuación, la codificación axial para agrupar y relacionar códigos en subcategorías emergentes; y finalmente, la triangulación de los hallazgos con la información documental. A partir de esta integración de fuentes, se elaboraron narrativas analíticas que articulan los resultados con los

[286] A excepción de "Patricia", usuaria de *Worldcoin*, que fue entrevistada en agosto de 2024.
[287] La persona entrevistada, usuaria de *Worldcoin*.

objetivos de conocer la situación, determinar impactos y proponer mecanismos de exigibilidad. De esta manera se asegura la coherencia, la validez interna y la riqueza interpretativa del estudio.

Por último, este estudio se rigió por los principios éticos de investigación, garantizando el consentimiento informado de todos los y las participantes. Previo a su participación, se les explicó el propósito de las entrevistas y se recabó su autorización expresa. Asimismo, se respetó en todo momento su derecho a retirarse del estudio sin consecuencia alguna. En el caso particular de la usuaria de *Worldcoin* (identificada como posible víctima) se preservó su anonimato mediante el uso de un seudónimo, protegiendo así su identidad. Adicionalmente, se cuidó la fidelidad de los testimonios, evitando interpretaciones sesgadas y respetando el contexto original de sus declaraciones.

## 2.1. Categoría 1: Impacto del entorno digital en la salud mental de niños, niñas y adolescentes

En esta primera categoría se explora cómo la inmersión de niños, niñas y adolescentes en el entorno digital incide de manera profunda y multifacética en su salud mental. A través de cinco subcategorías (sexualización, ansiedad y depresión, hiperconsumo, violencia digital e hiperconectividad e interacción social) se analizan los mecanismos y dinámicas que facilitan la exposición temprana a contenidos inapropiados, alimentan comparaciones dañinas, promueven conductas de consumo acrecentadas y potencian formas anónimas de acoso. Asimismo, se aborda la transición de las relaciones presenciales al plano virtual, sus implicaciones en el desarrollo emocional y los factores que agravan estas problemáticas, como la falta de acompañamiento psicosocial, la carencia de límites en el uso de dispositivos y la insuficiente rendición de cuentas de las plataformas digitales. Este análisis busca comprender no solo el impacto aislado de cada fenómeno, sino también su interacción y las condiciones estructurales que amplifican los riesgos para la salud mental de la población joven.

### 2.1.1. Subcategoría 1: Sexualización

Emilio Salao Sterckx[288] señala que durante la adolescencia, la exposición a los dispositivos digitales puede causar problemas en el desarrollo psicosexual,[289] ya que el entorno digital fomenta la satisfacción inmediata de deseos, lo que obstaculiza el desarrollo de habilidades para enfrentar situaciones que requieren paciencia y esfuerzo.[290] Este punto es complementado por Henry Zaruma,[291] quien ha observado un comportamiento sexualizado en niños y niñas de 8 a 10 años, debido al acceso a contenidos pornográficos a través de dispositivos digitales:

> Vamos con niños un poco más grandes como de ocho a diez años. Sucedió que estos niños, como pasaban la mayor parte de su tiempo utilizando un computador, celular, **tuvieron acceso a un montón de información y parte de esta información fue de contenido pornográfico**. Entonces nosotros cuando regresábamos a los colegios se veía que sus **comportamientos estaban muy sexualizados, en situaciones de juegos, que podían verse desde la mirada del adulto no apropiadas a su edad**, pero estaban exacerbadas estas conductas porque cuando se notaba, y no solamente en videos contenidos explícitos sino hasta en la música, porque venían con el reggaetón y esto es algo que ha influido.[292]

### 2.1.2. Subcategoría 2: Ansiedad y depresión

En la misma línea, Zaruma menciona que el acceso constante a redes sociales en adolescentes puede llevar a problemas de ansiedad y depresión, siendo las mujeres especialmente vulnerables debido a las comparaciones con la imagen femenina que se exhibe en línea, lo que puede causar trastornos alimenticios.[293] Ocaña hace referencia a una página web empleada por estudiantes en la que también se manifiestan expresiones de violencia digital que, en numerosas ocasiones, trascienden al ámbito físico: "Por los 'Confiésate' ha habido situaciones bastante graves, incluso en donde ha habido intentos de suicidio por el acoso tan grande las víctimas… Si he tenido situaciones de intentos de suicidio por la carga emocional que implica esto".[294]

---

[288] Psicólogo clínico, terapeuta y coordinador de vinculación con la colectividad del Instituto de Salud Pública de la Pontificia Universidad Católica del Ecuador.

[289] Emilio Salao Sterckx, "¿A qué edad los niños deben usar dispositivos digitales?", *Conexión PUCE*, 27 de mayo de 2022, https://conexion.puce.edu.ec/a-que-edad-los-ninos-deben-usar-dispositivos-digitales/, 3.

[290] Anexo 4, ver entrevista de Salao.

[291] Psicólogo en el Departamento de Consejería Estudiantil de la Unidad Educativa Bilingüe Julio Verne, estudiante de la maestría en adolescencia y Juventud de la Universidad Andina Simón Bolívar, sede Ecuador.

[292] Anexo 4, ver entrevista de Zaruma, El resaltado es propio del autor.

[293] Ibíd.

[294] Anexo 4, ver entrevista de Ocaña. El resaltado es propio del autor.

El uso excesivo de las redes sociales puede afectar negativamente la salud mental, generando una percepción pesimista de la vida. Esto se explica en parte porque los algoritmos tienden a priorizar la difusión de contenidos negativos, lo que expone constantemente a los usuarios y usuarias a este tipo de información. [295] En Ecuador, estadísticas del Ministerio de Salud Pública revelan que el 20% de niños, niñas y adolescentes presenta síntomas de depresión o ansiedad, y un 10% ha considerado o intentado suicidarse.[296] Estas alarmantes cifras, que han ido en aumento, podrían estar relacionadas con el creciente acceso a Internet entre este grupo etario.

En otros países ya se han presentado demandas a empresas de datos por dañar la salud mental de los niños a sabiendas. Entre 2011 y 2021, los casos de depresión entre adolescentes en Estados Unidos se duplicaron, un fenómeno atribuido al impacto de las redes sociales, según Jean Twenge, profesora de psicología de la Universidad Estatal de San Diego. Así, en octubre de 2023, 41 Estados de Estados Unidos presentaron una demanda contra *Meta*, la empresa matriz de *Facebook* e *Instagram*, acusándola de diseñar productos adictivos y perjudiciales para los niños, niñas y adolescentes. La denuncia alega que *Meta* manipula a los adolescentes mediante algoritmos y viola leyes federales de privacidad al recopilar datos sin consentimiento parental.[297]

### 2.1.3. Subcategoría 3: Hiperconsumo

Las redes sociales promueven una lógica de hiperconsumo que impacta especialmente en niños, niñas y adolescentes, quienes, al verse expuestos a contenidos

---

[295] DW Español [@dw_espanol], "Cómo las redes sociales enturbian nuestra visión del futuro El uso excesivo de las redes sociales puede afectar a nuestra salud mental y llevarnos a una visión sombría de la vida. Así es como puedes evitarlo. #DWDigital #DWMagacines https://t.co/uZXBi3pZdS", *Twitter*, 13 de mayo de 2024, https://x.com/dw_espanol/status/1790124198989385879.

[296] World Vision, Ministerio de Educación, y Red Nacional de Niñas, Niños, Adolescentes y Jóvenes Wamprakunapak Yuyaykuna, «Segunda Encuesta Nacional: "Tu voz, tus derechos". Sobre salud mental de niñas, niños, adolescentes y jóvenes», 2023, https://worldvisionamericalatina.org/ec/sala-de-prensa/salud-mental-en-ninos-ninas-y-adolescentes-en-ecuador-7-de-cada-10-se-sienten-felices-pero-el-20-enfrenta-dificultades-para-identificar-tristeza-y-estres, 2; Primicias, «La salud mental de los niños en Ecuador está marcada por los contrastes», *Primicias*, 5 de julio de 2023, https://www.primicias.ec/noticias/sociedad/ninos-salud-mental-depresion-acoso/, párr. 8; World Vision, "Salud mental en niños, niñas y adolescentes en Ecuador: 7 de cada 10 se sienten felices, pero el 20% enfrenta dificultades para identificar tristeza y estrés", accedido 29 de abril de 2025, https://worldvisionamericalatina.org/ec/sala-de-prensa/salud-mental-en-ninos-ninas-y-adolescentes-en-ecuador-7-de-cada-10-se-sienten-felices-pero-el-20-enfrenta-dificultades-para-identificar-tristeza-y-estres, párr. 4.

[297] La Vanguardia, "EE.UU. denuncia a Facebook e Instagram por dañar la salud mental de los niños a sabiendas", *La Vanguardia*, 26 de octubre de 2023, 2, 3, 4 8, 10, https://www.lavanguardia.com/vida/20231026/9329037/eeuu-denuncia-facebook-instagram-danar-salud-mental-ninos-sabiendas.html.

idealizados, internalizan modelos de vida, cuerpos y objetos como metas deseables. Esta constante comparación con los estándares difundidos en redes sociales genera inseguridades que muchas veces se intentan compensar mediante el consumo de productos, reforzando así una dinámica mercantil que se alimenta de estas carencias afectivas y simbólicas. Uno de los psicólogos entrevistados advierte sobre esta relación entre redes sociales, vulnerabilidad adolescente y consumo exacerbado:

> Entonces cuando los chicos ven un video en TikTok o en cualquier red social, aparece este fenómeno de la comparación: 'Yo no tengo este cuerpo', 'Yo no tengo esta casa', 'Yo no tengo estas cosas', y los chicos entran en esta lógica de consumir y seguir reproduciendo esta matriz productiva [...], el sistema económico que está sustentando esto se ve beneficiado [...] pero ¿a qué costo? A todo este costo que como psicólogos observamos con los chicos. [298]

Desde esta perspectiva, las redes sociales no solo funcionan como plataformas de comunicación, sino como engranajes de una economía que explota los datos personales y las inseguridades adolescentes para fomentar el hiperconsumo. Este fenómeno se ve atravesado también por variables como el género, dado que los estereotipos impuestos afectan de manera diferenciada a mujeres adolescentes y refuerzan mandatos corporales asociados al ideal femenino, lo que se traduce en trastornos alimentarios, problemas de autoimagen y presiones constantes por alcanzar modelos inalcanzables promovidos desde el entorno digital.

### 2.1.4. Subcategoría 4: Violencia Digital

Fernando Ocaña,[299] psicólogo entrevistado, introduce el tema de la violencia digital, señalando que ha aumentado en los últimos años y es difícil identificar a los responsables. Cita ejemplos de estudiantes que utilizan plataformas anónimas para promover el acoso y la violencia, lo que ha resultado en problemas de acoso e intentos de suicidio:

> "Confiésate" es una Fan Page que crean los estudiantes anónimos porque nunca ponen su identificación para que sus compañeros compartan chismes, declaraciones, imágenes, memes ofensivos, es decir, que compartan todo lo que les da la gana. Y hay una premisa principal en todos los "Confiésate", es una palabra que los jóvenes utilizan: en cada post que hacen en los "Confiésate" al final ponen "TAPA". Yo no entendía desde mi diferencia generacional, lo asemejaba al "tapa" de "tonto", y el "TAPA" ha sido el "no digas quien soy", porque ellos a la Fan Page mandan mensajes para que publiquen el mensaje, pero

[298] Anexo 4, ver entrevista de Henry Zaruma.

[299] Psicólogo Clínico, especialista en educación y nuevas tecnologías de comunicación e información por la Universidad Andina Simón Bolívar. Analista del Departamento de Consejería Estudiantil de la Unidad Educativa Aviación Civil.

> les ponen que no divulguen quien es. **El que maneja la página nunca se muestra porque sabe sobre las graves consecuencias que tendrá, porque está promoviendo violencia, peleas**. Donde publican peleas, chismes, que promueve a que en el recreo se agarren a la entrada y salida, se insulten, amenacen, se agreden […] **la violencia digital se ha incrementado de manera increíble**. Puedo poner un antes y un después de la Pandemia, si había violencia digital, pero después de la pandemia, donde nos hemos arrojado todos un poco más a la virtualidad, se ha incrementado exponencialmente. **Es un incremento generacional e increíble de la violencia**.[300]

La violencia digital entre adolescentes se ha vuelto más común y difícil de controlar, especialmente por el anonimato que ofrecen ciertas plataformas. Como explica Ocaña, páginas como "Confiésate" permiten que los estudiantes publiquen chismes, insultos y amenazas sin dar la cara, lo que genera conflictos dentro y fuera del entorno escolar. Esta forma de violencia no solo afecta la convivencia, sino que también puede tener graves consecuencias en la salud mental de los jóvenes, como ansiedad, depresión e incluso intentos de suicidio. Por eso, es importante entender que la violencia digital no se queda solo en las redes, sino que impacta directamente en la vida real de niños, niñas y adolescentes.

### 2.1.5. Subcategoría 5: Hiperconectividad e Interacción Social

El entorno digital también transformó profundamente la forma en que niños, niñas y adolescentes interactúan socialmente. Las restricciones de movilidad y el distanciamiento físico llevaron a una migración casi total de las relaciones sociales hacia entornos digitales. Según UNICEF, la pandemia privó a los adolescentes de pasar tiempo con sus pares y de participar en actividades educativas, culturales y deportivas, desplazando su experiencia social al plano virtual.[301]

En este contexto, el psicólogo Fernando Ocaña señala cómo esta transición ha normalizado la interacción digital en edades cada vez más tempranas:

> He podido constatar que las relaciones de este grupo poblacional se están basando ahora exclusivamente en aspectos digitales, principalmente de las redes sociales. No es raro ya ver a niños, niñas desde los 10 años más o menos, que ya tienen redes sociales, que

---

[300] Anexo 4, ver entrevista de Ocaña. El resaltado es propio del autor.

[301] Unicef, "Cinco formas en que la pandemia impactó a los adolescentes", 2021, https://www.unicef.org/uruguay/crianza/adolescencia/cinco-formas-en-que-la-pandemia-impacto-los-adolescentes, párr. 3; Unicef, "Aumenta la preocupación por el bienestar de los niños y los jóvenes ante el incremento del tiempo que pasan frente a las pantallas, según UNICEF", 4 de febrero de 2021, https://www.unicef.org/lac/comunicados-prensa/aumenta-la-preocupacion-por-el-bienestar-de-los-ninos-y-los-jovenes-ante-el-incremento-del-tiempo-frente-a-las-pantallas.

> chatean con sus compañeros, que están en ciertos grupos, y claro, **se basa mucho ahora su interrelación con estos medios digitales**.[302]

Ocaña destaca que si bien este fenómeno es en parte esperable debido a los avances tecnológicos y a los patrones de aprendizaje por imitación dentro del entorno familiar, también advierte que las consecuencias de no saber manejar adecuadamente esta hiperconectividad son preocupantes: "Ahora, las consecuencias que trae no manejarlo, es otra cosa."[303]

Por su parte, la psicóloga Emilia Piedra[304] aporta un caso concreto que ilustra los efectos de esta hiperconexión en la salud mental de las y los adolescentes. Describe cómo una niña desarrolló una fuerte dependencia del celular y de sus interacciones virtuales, al punto de experimentar ansiedad intensa por no responder mensajes a tiempo:

> [...] las personas con las que interactuaba eran virtuales, es decir, sus amigos eran de otros lugares, se contactaban a través del celular […] el hecho de que a veces ella sienta esta **ansiedad de que no está respondiendo a tiempo,** de que debería estar ahí, a veces **le generaba angustia y sobre todo malestar el hecho de estar constantemente teniendo que estar pendiente más en el celular** [...] más que estar en el 'aquí', en el presente, en la parte real […] **Era como tener una segunda vida; estar aquí y en la pantalla**.[305]

Estas experiencias son consistentes con estudios recientes que demuestran que darles a los niños y niñas dispositivos digitales para apaciguar sus enojos afecta al desarrollo de sus habilidades para el manejo de la frustración y la ira, lo que lleva a un peor control y manejo de la ira en el niño o niña, y aumenta la probabilidad de la dependencia a dispositivos digitales.[306]

### 2.2. Categoría 2: Pandemia y Virtualidad

Todas los participantes entrevistados manifestaron que La pandemia de COVID-19 marcó un antes y un después en la virtualidad de los niños, niñas y adolescentes debido a varios factores clave que transformaron su vida cotidiana y su interacción con la tecnología:

---

[302] Anexo 4, ver entrevista de Ocaña, El resaltado es propio del autor.

[303] Ibíd.

[304] Licenciada en Psicología, ha trabajado con niños y niñas de 2 a 6 años y con la organización Akuankuna para prevenir la violencia en niños, niñas y adolescentes.

[305] Ibíd, ver entrevista de Piedra, El resaltado es propio del autor.

[306] V. Konok et al., "Cure for Tantrums? Longitudinal Associations between Parental Digital Emotion Regulation and Children's Self-Regulatory Skills", *Frontiers in Child and Adolescent Psychiatry* 3 (2024): 1276154, doi:10.3389/frcha.2024.1276154, 9.

> […] un punto clave que si marca la diferencia de eso es precisamente la pandemia del COVID-19. **Antes de la pandemia había unas necesidades específicas que eran muy notorias en el espacio de consulta y después de la pandemia se presentaron otras, o se retoman esas mismas demandas, pero ya con otros elementos importantes que sí invitan a la reflexión**[…] La pandemia marcó preocupaciones que empiezan a distinguirse o que son diferentes a las que existía antes de la pandemia[…] siempre que se trata de hablar sobre la situación de la niñez y adolescencia en el Ecuador no se puede dejar de lado el tema de la pandemia porque si **marca un antes y un después sobre la salud mental de la población más joven del Ecuador**.[307]

Este cambio profundo se debe, en gran parte, a la intensificación del uso de dispositivos electrónicos y redes sociales durante el confinamiento, lo que generó nuevas formas de interacción, pero también nuevos riesgos. El aislamiento, la sobreexposición a pantallas y la dependencia del entorno digital para socializar y estudiar alteraron significativamente el desarrollo emocional y psicológico de niños, niñas y adolescentes. Los efectos de este periodo aún se evidencian en el aumento de casos de ansiedad, depresión y dificultades para establecer vínculos afectivos saludables, lo que demuestra que la virtualidad impuesta por la pandemia no solo transformó las dinámicas educativas, sino que también tuvo un fuerte impacto en la salud mental de esta población.

### 2.2.1. Subcategoría 1: Educación virtual

Uno de los cambios más profundos provocados por la pandemia fue en el ámbito educativo. La necesidad de continuar con la enseñanza llevó a una adopción apresurada y generalizada de plataformas virtuales. Escuelas y universidades tuvieron que adaptarse de forma casi inmediata, lo que obligó tanto a docentes como a estudiantes a adquirir habilidades digitales y dispositivos tecnológicos para poder mantenerse conectados. Esta transición, sin una preparación previa adecuada, evidenció brechas tecnológicas y socioeconómicas en muchas familias:

> Tengo que hablar que se 'lanzó' [la educación virtual] porque nadie estábamos preparados para la virtualidad, nadie. Ni los docentes, ni los mismos estudiantes, entonces se vieron obligados a buscar formas de obtener este recurso: sea por donaciones, por préstamos o sea que se endeudaron algunas personas porque necesitaban acceder, porque **sus hijos prácticamente muchos aprendían desde el celular**. Y también eso marcó la necesidad del internet, porque claro, no servía de nada tener el celular si no tenían internet.[308]

Esta situación marcó no solo un cambio en el uso de herramientas tecnológicas, sino también una acelerada inmersión en el mundo digital que dejó efectos duraderos en la dinámica educativa y familiar.

---

[307] Anexo 4, ver entrevista de Salao, El resaltado es propio del autor.
[308] Ibíd, ver entrevista de Fernando Ocaña, El resaltado es propio del autor.

Estas afirmaciones concuerdan con estudios realizados por Unicef y el Ministerio de Educación durante la pandemia, que exponen las dificultades de los NNA en la educación virtual. Por ejemplo, se establece que el 86,5 % de los hogares de estudiantes contaba con conexión a internet durante la pandemia, pero 5 de cada 10 estudiantes no disponían de computadora y sólo 2 de cada 10 tenían un dispositivo de uso personal, lo que, junto con la mala calidad de la conectividad, generó que el 24,9 % de los NNA no se concentrara, el 21,5 % no comprendiera las clases y el 18,7 % señalara la conectividad como principal obstáculo;[309] a ello se sumó un abandono escolar que, aunque bajo a nivel nacional, llegó al 4,7 % en la educación intercultural bilingüe[310] y pérdidas de aprendizaje percibidas por 8 de cada 10 docentes que consideraron que sus estudiantes aprenden menos o nada.[311] Las condiciones socioeconómicas también se deterioraron: cerca de 1 de cada 3 hogares continuaba necesitando asegurar alimentos suficientes.[312]

### 2.2.2. Subcategoría 2: Salud emocional y física

Durante la pandemia, la salud emocional y física de niños, niñas y adolescentes se vio gravemente afectada por el aislamiento, la incertidumbre y el cambio abrupto en sus rutinas. El confinamiento prolongado y la interrupción de actividades presenciales intensificaron sentimientos de ansiedad, estrés y tristeza en esta población. Según datos recogidos durante la emergencia sanitaria, el 40,7 % de los NNA en Ecuador reportó sentirse muy angustiado o tensionado, mientras que docentes identificaron como principales riesgos psicosociales la depresión, la desmotivación y la falta de apoyo familiar.[313]

Ante este panorama, en Ecuador, el Ministerio de Salud Pública puso en marcha la línea telefónica 171, destinada a ofrecer atención psicológica a distancia. Esta estrategia buscó ampliar la contención emocional ante el aumento de afecciones en la salud mental de la población, especialmente durante el aislamiento y el proceso de adaptación a la "nueva normalidad".[314]

---

[309] Unicef y Ministerio de Educación, "Resultados de las encuestas de monitoreo del impacto de la pandemia de COVID-19 en la comunidad educativa ecuatoriana", 2022, https://www.unicef.org/ecuador/media/10156/file/Ecuador_encuestas_covid_educacion.pdf.pdf, 71.

[310] Ibíd, 93.

[311] Ibíd, 49.

[312] Ibíd, 101.

[313] Unicef y Ministerio de Educación, "Resultados de las encuestas de monitoreo del impacto de la pandemia de COVID-19 en la comunidad educativa ecuatoriana", 39.

[314] Ecuador, Presidencia, "Más de 82.000 personas recibieron atención en salud mental durante la Emergencia Sanitaria – Presidencia de la República del Ecuador", s.f.,

En este contexto, Ocaña advierte que uno de los impactos más visibles en adolescentes ha sido el deterioro de la autoestima, influenciado por la exposición a estándares irreales de belleza en redes sociales:

> La situación de problemas de autoestima también ha crecido bastantísimo porque es mucho más sencillo proyectar una imagen digital, porque ahora tenemos filtros: filtros que cambian, que ocultan ciertas características, ciertos aspectos que puede que no me agraden de mi físico, y priorizo mostrarme desde ahí, pero de forma presencial, es decir cara a cara, no lo hago. Esto también se arrastró con la pandemia, **los niños, niñas y adolescentes ahora priorizan el uso de la mascarilla, pero no es por situaciones de salud, es por situación de problemas de autoestima**, en donde **no quieren desprenderse de la mascarilla porque no quieren que vean su rostro** cien por ciento, **piensan que su rostro no es atractivo o puede ser motivo de burlas** y demás, pero en cambio en redes sociales sí se muestran con todos los filtros que puedan utilizar.[315]

Al mismo tiempo, el confinamiento obligó a muchas familias a vivir en espacios reducidos, aumentando la exposición de NNA a contextos de violencia doméstica y estrés familiar. En zonas urbanas de América Latina, el 51,2 % de los niños, niñas y adolescentes habita en condiciones de precariedad habitacional, y más de 18 millones viven en hogares con condiciones de habitabilidad extremadamente deficientes.[316] Esta situación intensificó su vulnerabilidad emocional y física durante el encierro.

Por otro lado, el uso intensivo de tecnología durante la pandemia generó consecuencias en la salud física. Si bien permitió la continuidad educativa y el desarrollo acelerado de habilidades digitales, también se asoció con efectos negativos como fatiga visual, sedentarismo y alteraciones del sueño, derivados del exceso de tiempo frente a pantallas.[317]

### 2.2.3. Subcategoría 3: Brecha Digital

Por último, la pandemia evidenció y, en muchos casos, profundizó la brecha digital, revelando las desigualdades existentes en el acceso a la tecnología y la conectividad:

---

https://www.presidencia.gob.ec/mas-de-82-000-personas-recibieron-atencion-en-salud-mental-durante-la-emergencia-sanitaria/, párrs. 2-3.

[315] Anexo 4, ver entrevista de Ocaña, El resaltado es propio del autor.

[316] CEPAL y UNESCO, "La educación en tiempos de la pandemia de COVID-19", agosto de 2020, https://repositorio.cepal.org/server/api/core/bitstreams/c29b3843-bd8f-4796-8c6d-5fcb9c139449/content, 13-14.

[317] Equipo Médico de SaludOnNet, "¿Cómo afecta en la salud mental y física el uso excesivo de pantallas?", *Blog SaludOnNet*, 3 de octubre de 2024, https://www.saludonnet.com/blog/como-afecta-en-la-salud-mental-y-fisica-el-uso-excesivo-de-pantallas/, párrs. 3-7.

> Normalmente es **en la etapa de la adolescencia en donde los chicos, en el proceso de la configuración de la identidad, perciben mucho más las diferencias de clases sociales**. […] el Internet supuestamente está colocado en el mundo para que nos podamos conectar entre todos, para que podamos liberar la información y tener acceso en igual de condiciones a todos, pero en realidad **lo que observamos es que el Internet en realidad promueve con estas brechas de acceso es una mayor desigualdad, y esto se traduce en las relaciones sociales entre niños, niñas y adolescentes**. […] **Los niños que no tienen ahorita Internet probablemente en el futuro van a tener menos capacidad de participación social,** menos acceso a la información y por ende tal vez menos oportunidades.[318]

Estas brechas se ampliaron en varios grupos: se registró una diferencia de -2,8 puntos porcentuales entre áreas rurales y urbanas, 1,3 puntos a favor de las mujeres frente a los hombres, 2,5 puntos a favor de los mestizos respecto a los pueblos indígenas, y 4,7 puntos a favor de los estudiantes de mayores ingresos en comparación con los de menores recursos.[319] Aunque se impulsaron esfuerzos importantes para dotar de dispositivos y conexión a estudiantes en situación de vulnerabilidad, las desigualdades persistieron. No obstante, la educación, el trabajo y la interacción social en entornos virtuales han terminado por consolidarse como parte de la "nueva normalidad."[320]

Tabla 5
**Impactos psicosociales de la pandemia en NNA**

| Dimensión afectada | Impactos |
|---|---|
| Concentración y comprensión | Dificultad para concentrarse y menor comprensión de las clases |
| Ansiedad y estrés | Percepción de angustia y tensión |
| Interacción social | Aislamiento llevó al uso de redes sociales para socializar |
| Apoyo familiar y emocional | Docentes reportan desmotivación, tristeza, falta de apoyo |
| Condiciones de vivienda | Precariedad habitacional |
| Salud física (sueño, sedentarismo, visión) | Fatiga visual, sedentarismo, problemas de sueño |
| Brecha digital y desigualdad | Aumentó la brecha digital según ingreso, nacionalidad y zona geográfica |

Fuente: Anexo 4
Elaboración propia, 2025

En conclusión, la pandemia y la virtualidad transformaron profundamente la vida de niños, niñas y adolescentes, afectando múltiples dimensiones de su desarrollo. La rápida adopción de la educación en línea evidenció y amplificó las desigualdades en el acceso a tecnología y conectividad, generando dificultades de aprendizaje, desconexión emocional y pérdida de vínculos escolares. A esto se sumaron el aislamiento social, el

[318] Anexo 4, Ver entrevista de Salao, El resaltado es propio del autor.
[319] INEC Ecuador, "Desigualdades Educativas en el contexto de la pandemia de la COVID-19 en el Ecuador", junio de 2022, https://www.ecuadorencifras.gob.ec/documentos/web-inec/Bibliotecas/Libros/Reportes/Educacion_COVID.pdf, 29.
[320] Unicef y Ministerio de Educación, "Resultados de las encuestas de monitoreo del impacto de la pandemia de COVID-19 en la comunidad educativa ecuatoriana", 101.

incremento de la ansiedad y el estrés, y un entorno familiar y habitacional en muchos casos precario. Aunque se desarrollaron nuevas habilidades digitales y se implementaron medidas de apoyo psicosocial, los impactos negativos sobre la salud mental, el bienestar físico y la equidad educativa han dejado una huella duradera en esta generación.

### 2.3. Categoría 3: Corresponsabilidad en el entorno digital

Esta categoría examina la corresponsabilidad de tres actores fundamentales en la protección de la infancia y adolescencia en entornos digitales. En primer lugar, la familia debe asumir un papel activo en la alfabetización digital de sus miembros más jóvenes, estableciendo normas de uso razonables y supervisando el acceso a dispositivos y plataformas, tal como se advierte al señalar la necesidad de formarse para "combatir los problemas que crea el mal uso de las herramientas digitales" mediante una adecuada preparación parental.

En segundo lugar, el Estado debe garantizar el acceso universal a servicios de salud mental y desarrollar políticas públicas de educación mediática que operativicen las disposiciones legales existentes, dotando a las autoridades de mecanismos efectivos de rendición de cuentas. Finalmente, las empresas tecnológicas tienen la obligación de diseñar controles de tiempo, transparencia en el tratamiento de datos y programas de formación sobre riesgos psicosociales, superando la mera autorregulación para responder a su responsabilidad social. Solo a través de la articulación coordinada de estos tres ámbitos será posible mitigar los riesgos y promover un entorno digital seguro y saludable para niños, niñas y adolescentes.

#### 2.3.1. Subcategoría 1: Rol de la familia

Salao y Zaruma consideran que el uso extendido de dispositivos digitales en niños y niñas responde más a las necesidades de los padres que a las de los niños o niñas, siendo una forma de calmar el llanto y proporcionar distracción.[321] En la misma línea, se considera que "antes de los cinco años, los niños y niñas necesitan una conexión con la realidad mucho más social".[322]

[321] Anexo 4, ver entrevistas de Salao y Zaruma.

[322] Emilio Salao Sterckx, "¿A qué edad los niños deben usar dispositivos digitales?", Conexión *PUCE*, 27 de mayo de 2022, https://conexion.puce.edu.ec/a-que-edad-los-ninos-deben-usar-dispositivos-digitales/, 7.

Sin embargo, la vida moderna, caracterizada por padres multitarea y ocupaciones laborales, ha incrementado esta dependencia tecnológica. Controlar el uso de dispositivos digitales es complicado debido a la falta de regulación y la prevalencia de hábitos tecnológicos descontrolados en la sociedad. Es crucial desarrollar la capacidad de autorregulación y establecer normas de uso desde una edad temprana. Ocaña afirma que "Los padres deberían educarse. No podemos combatir los problemas que crea el mal uso de las herramientas digitales si no estamos completamente preparados y conocemos qué es y cómo se utiliza (…) lamentablemente hay una gran cantidad de personas de generaciones arriba que son analfabetas digitales."[323]

Para niños mayores de cinco años, se recomienda limitar el uso de smartphones a una o dos horas diarias, estableciendo hábitos digitales regulados.[324] Con respecto a las y los adolescentes, el acceso a redes sociales debería basarse en su capacidad para discernir entre lo adecuado y lo inapropiado.[325]

### 2.3.2. Subcategoría 2: Rol del Estado

La solución no debe recaer únicamente en los padres de familia. Los estados deberían garantizar el acceso a la salud mental y priorizar la prevención a través de la educación; sin embargo, en el Ecuador el acceso a la atención psicológica sigue siendo un privilegio y la educación sobre Internet y redes sociales sigue siendo escasa.[326]

También es necesario que la normativa nacional otorgue mayores facultades al Estado para que ordene la rendición de cuentas a las empresas de datos:

> Me parece que las legislaciones de los estados, especialmente de países latinoamericanos como el Ecuador, puedan poner por encima de los intereses económicos de estas empresas las leyes con las que regulan las relaciones con sus ciudadanos, sea la prioridad. Entonces a una empresa no se le puede pedir tomar sensibilidad sobre las necesidades de una población o las prioridades de salud pública porque no lo van a hacer. Pero creo que **en las normas nacionales e internacionales se les dé más autoridad a los países para poder controlar y pedir que rindan cuentas estas organizaciones por las acciones de sus países**.[327]

En este sentido, resulta urgente fortalecer la legislación y la institucionalidad pública para que el Estado no solo actúe como garante de derechos, sino también como

[323] Anexo 4, ver entrevista de Ocaña.
[324] Anexo 4, ver entrevista de Salao.
[325] Ibíd.
[326] Anexo 4, Ver entrevista de Zaruma.
[327] Ibíd, Ver entrevista de Salao, el resaltado es propio del autor.

regulador activo frente al poder de las plataformas digitales. Solo así será posible equilibrar la balanza entre el bienestar de las poblaciones más vulnerables, como niños, niñas y adolescentes, y los intereses económicos de las corporaciones tecnológicas.

### 2.3.3. Subcategoría 3: Rol de las Empresas

Las personas entrevistadas coinciden en que las empresas de datos no tienen controles adecuados, y considerar su autorregulación "es como pedirle al lobo que no se coma a las ovejas",[328] ya que sus intereses económicos suelen estar por encima del bienestar de los usuarios, especialmente de los más vulnerables como niños, niñas y adolescentes. Además, establecen que las empresas deberían tener un compromiso mucho más fuerte con la salud mental. Al respecto Piedra menciona que:

> Las empresas deberían poner más controles, como, por ejemplo, límites de tiempo a los niños, niñas y adolescentes. Asimismo, **deberían educar a las personas consumidoras de sus servicios sobre los impactos en la salud mental que podría generar su consumo**. He observado de cerca las dinámicas de uso de dispositivos digitales en niños pequeños. Éstos están expuestos a contenido que puede ser dañino para su salud mental. […] Todas estas cosas deberían ser debidamente informadas, tanto a los cuidadores como a los niños y niñas.[329]

Resulta evidente que la protección de la salud mental infantil no puede dejarse al criterio de empresas cuyo principal objetivo es maximizar ganancias. Es imprescindible que los Estados asuman un rol activo y regulador, estableciendo límites claros, fomentando la educación digital desde edades tempranas y exigiendo mayor transparencia y responsabilidad a las plataformas tecnológicas. Solo mediante una acción conjunta entre gobiernos, sociedad civil y sector privado será posible garantizar entornos digitales más seguros y saludables para las nuevas generaciones.

## 2.4. Categoría 4: Protección de datos personales de Niños, Niñas y Adolescentes

En esta cuarta categoría se analiza la protección de datos personales de niños, niñas y adolescentes, entendida como un eje fundamental para preservar su privacidad e integridad en el entorno digital. A través de la subcategoría de riesgos en redes sociales e identidad digital se examina cómo la huella de datos (fotos, comentarios, geolocalización) construye perfiles vulnerables, tanto por la exposición temprana de NNA sin percepción del riesgo como por prácticas de *sharenting* que pueden derivar en acoso o grooming.

---

[328] Ibíd, Ver entrevista de Zaruma.
[329] Ibíd, Ver entrevista de Piedra, El resaltado es propio del autor.

La subcategoría de legislación vigente revisa el marco normativo reforzado y sus carencias prácticas, a la luz de la crítica de un enfoque empresarial que ha desatendido aportes de la sociedad civil. En políticas públicas se evalúa la limitada vigencia de la "Internet Segura" y la ausencia de iniciativas activas, mientras que la de instituciones describe el despliegue reciente de la Superintendencia de Protección de Datos Personales, sus primeras resoluciones y retos para cumplir con su mandato de supervisar, sancionar y orientar sobre el tratamiento de datos de NNA.

### 2.4.1. Subcategoría 1: Riesgos en redes sociales e identidad digital

De acuerdo con Lorena Naranjo,[330] al utilizar la web, buscadores, redes sociales, juegos en línea, aplicaciones móviles, plataformas, y servicios públicos y privados a través de canales digitales, se deja una huella de información y datos. Esta huella digital se va enriqueciendo con fotos, videos, documentos, comentarios e interacciones que revelan aspectos de nuestra identidad como el rostro, el cuerpo, la voz, las ideas y pensamientos. Estos elementos van componiendo un retrato que narra quiénes somos, nuestro círculo familiar y social, nuestras preferencias, y cómo nos proyectamos en sociedad.[331]

Además, esta acumulación de información puede provenir también de internautas que publican datos sobre nosotros, asociándonos con imágenes, lugares y grupos que completan nuestra identidad digital. La gestión de la identidad digital y de la reputación en línea es una realidad actual que los adultos aprenden a manejar, a menudo, a través de las consecuencias de errores propios o ajenos. Sin embargo, los niños y niñas son especialmente vulnerables. En primer lugar, porque los padres pueden permitirles el acceso temprano a redes sociales, antes de que desarrollen una percepción adecuada del riesgo, exponiendo información sobre su familia, amistades, colegio e itinerarios que pueden ser utilizados por personas malintencionadas para dañarlos.[332]

En segundo lugar, los propios padres pueden incurrir en *sharenting* o sobreexposición, al publicar indiscriminadamente contenidos como videos, fotos y

---

[330] Lorena Naranjo Godoy es PhD en Ciencias Jurídicas, experta en derecho digital, protección de datos y ciberseguridad, con más de 20 años de experiencia en sectores público y privado. Fue autora y promotora de la Ley Orgánica de Protección de Datos Personales en Ecuador.

[331] Lorena Naranjo Godoy, "Internet segura para la niñez y adolescencia", *El Comercio*, 13 de mayo de 2024, párr. 1, https://www.elcomercio.com/opinion/internet-segura-para-ninez-adolescencia-lorena-godoy-columnista.html.

[332] Anexo 4, Ver entrevista de Naranjo Godoy.

anécdotas aparentemente inofensivas. Esto puede causar molestias e inseguridades a los niños y niñas, facilitar formas de acoso o incluso ponerlos en riesgo de ser víctimas de delitos como el *grooming*.[333]

Por su parte, los adolescentes, bajo presión social, pueden publicar contenido inapropiado relacionado con el consumo de alcohol, drogas, comentarios inadecuados y material sexual. En Ecuador, es común la creación de grupos en redes sociales de compañeros de clase donde se comparten contenidos ofensivos y denigrantes, prácticas conocidas como "ciberbullying", o se difunden fotos y videos sexuales que violan la intimidad.[334] Estos problemas requieren una actuación judicial para proteger a las víctimas y una respuesta coordinada por parte del Estado, que debe desarrollar la infraestructura, recursos y conocimientos necesarios para una respuesta inmediata y eficiente.

Así, es fundamental realizar esfuerzos de prevención, ya que niños, niñas y adolescentes están en proceso de construir su identidad y reputación digital. Padres, cuidadores y educadores deben informarse y educarse para orientar a los niños, niñas y adolescentes en la creación de una huella digital positiva en redes sociales, que beneficie sus vidas y relaciones presentes y futuras. Por lo tanto, es crucial aprender a navegar en línea de forma segura, y medir las consecuencias de la creación y participación en grupos, así como de la información que se sube, etiqueta o comenta.[335]

### 2.4.2. Subcategoría 2: Legislación vigente

Naranjo, quien impulsó la aprobación de la LOPDP cuando fue directora nacional de DINARDAP (ahora DINARP), menciona que los niños, niñas y adolescentes poseen un marco de protección reforzado dentro de la norma, pues se requiere su consentimiento explícito desde los 15 años, y si tienen menos se requiere la autorización expresa de su representante legal.[336]Además de esta protección, también se debe realizar una evaluación de impactos y se encuentra prohibido realizar análisis automatizados de sus datos personales.[337]

---

[333] Ibíd.

[334] Ibíd, Ver entrevista de Zaruma.

[335] Ibíd, Ver entrevista de Naranjo Godoy.

[336] Anexo 4, Ver entrevista de Naranjo Godoy; Ecuador, *Ley Orgánica de Protección de Datos Personales*, Registro Oficial 459, Suplemento, 26 de mayo de 2021, art. 24.

[337] Anexo 4, Ver entrevista de Naranjo Godoy.

De la misma forma, como se señala en el primer capítulo, la Ley Orgánica de Protección de Datos Personales desarrolla el derecho a la protección de datos personales en Ecuador. Sin embargo, de acuerdo con Ola Bini,[338] entrevistado por el autor, esta normativa no tiene un enfoque de derechos humanos, sino que ha sido desarrollada desde una perspectiva empresarial.

Al respecto, menciona que el Centro de Autonomía Digital (CAD), realizó un análisis sobre el Proyecto de Ley de Protección de Datos Personales en 2020, tomando como insumo las cartas enviadas de manera conjunta a la Asamblea Nacional por parte de las organizaciones de la sociedad civil como APC,[339] Derechos Digitales[340] y *Access Now*; no obstante, ninguno de estos comentarios fue incorporado, mientras que sí se incorporaron las observaciones de las cámaras de comercio y demás organizaciones que representan a las empresas.[341]

Entre las observaciones que se hicieron, se señaló que se consideraba importante que se cite como referente el RGPD, que en su artículo 83 ordena sanciones basadas en porcentajes del volumen de ventas anual del año anterior,[342] esto con el fin de establecer sanciones adecuadas conforme al tamaño de la empresa. Asimismo, con respecto al derecho a no ser objeto de una decisión basada únicamente en valoraciones automatizadas, señaló que es importante que se debe especificar que este tipo de decisiones representan la capacidad de decidir por medios tecnológicos sin la intervención del ser humano,[343] esto con el propósito de que se aclare las implicaciones que tiene este derecho.

Sobre las excepciones de consentimiento para la transferencia o comunicación de datos personales de la LOPDP, este análisis indica que es importante proteger la

---

[338] Ola Martin Gustafsson, es un desarrollador de software, programador y activista de Internet sueco. Desde 2013 reside en Ecuador, donde trabaja en el Centro de Autonomía Digital en temas relacionados con privacidad, seguridad y criptografía. En abril de 2019, fue detenido en Ecuador debido a su presunta vinculación con Julian Assange y Wikileaks. Su proceso penal continúa abierto. Su caso atrajo la atención internacional y planteó cuestiones sobre la libertad en línea y la protección de datos.

[339] Association for Progressive Communication es una red mundial de apoyo al uso de Internet y las TICs para la justicia social y el desarrollo sostenible. En "APC (@APC_News) / X", *X (formerly Twitter)*, 5 de junio de 2024, https://x.com/apc_news.

[340] Derechos Digitales es una organización de alcance latinoameroicano, independiente y sin fines de lucro, fundada en 2005 y que tiene como objetivo fundamental el desarrollo, la defensa y la promoción de los derechos humanos en el entorno digital. En "Derechos Digitales", *Derechos Digitales*, accedido 9 de noviembre de 2021, https://www.derechosdigitales.org/quienes-somos/derechos-digitales/.

[341] Anexo 4, Ola Bini, entrevistado por el autor, 1 de mayo de 2024.

[342] Anexo 5, Centro de Autonomía Digital, Análisis del Proyecto de Ley Orgánica de Protección de Datos Personales.

[343] Ibíd., 14.

información que se recolecta de fuentes de acceso público, porque la recolección masiva de estos datos pueden crear perfiles suficientes para vulnerar la privacidad de las personas sin su consentimiento, por lo que se debe eliminar la excepción de que no es necesario contar con el consentimiento del titular para la transferencia o comunicación de datos personales cuando éstos han sido recogidos desde fuentes accesibles al público.[344] Así es importante tener en consideración que la información accesible a través de fuentes abiertas incluye las publicaciones en redes sociales, información de sistemas estatales, publicaciones de prensa, entre otras.

Por último, Bini introduce elementos que se deberían considerar para que la norma tenga la fuerza suficiente de generar cambios reales en la protección de derechos, por lo que se debe establecer "Presupuesto para la superintendencia, (…) asegurar la independencia de las diferentes partes del gobierno; incluso entre el gobierno y empresas grandes. Cooperación internacional también. Necesitas una ley que tenga suficiente poder, pero los comercios no quieren esto"[345]

### 2.4.3. Subcategoría 3: Políticas Públicas

Lorena Naranjo y Paulina Casares Subia[346] señalan que en 2020 se creó en Ecuador la primera Política Pública para una Internet segura para niños, niñas y adolescentes. Este esfuerzo involucró a 22 instituciones estatales y de la sociedad civil,[347] con el objetivo de generar:

> Una política de uso sano, seguro y constructivo de internet, para niños, niñas y adolescentes parte de la intención de potenciar las oportunidades y habilidades que

---

[344] Ibíd., 17.

[345] Anexo 4, Ver entrevista de Bini.

[346] Directora de Control y Vigilancia de Mercado en el Ministerio de Producción, Comercio Exterior, Inversiones y Pesca. Fue parte de la terna enviada por el presidente Noboa al Consejo de Participación Ciudadana y Control Social para que se elija al primer Superintendente de Protección de Datos (conforme al art. 77 de la LOPDP).

[347] Ministerio de Educación, Ministerio de Gobierno, Ministerio de Inclusión Económica y Social, Ministerio de Relaciones Exteriores y Movilidad Humana, Ministerio de Telecomunicaciones y de la Sociedad de la Información, Secretaría de Derechos Humanos, Consejo Nacional para la Igualdad Intergeneracional, Dirección Nacional de Registro de Datos Públicos, Instituto Nacional de Estadística y Censos, Agencia de Regulación y Control de las Telecomunicaciones, Consejo de Regulación y Control de las Telecomunicaciones, Consejo de Regulación, Desarrollo y Promoción de la Información y Comunicación, Consejo de la Judicatura, Fiscalía General del Estado, Asociación de Municipalidades Ecuatorianas, Consorcio de Gobiernos Autónomos Provinciales del Ecuador (Congope), Centro Internaicional de Estudios Superiores de Comunicaicón para América Latina (Ciespal), Corporación Nacional de Telecomunicaciones, Asociación Ecuatoriana de Ciberseguridad, Childfund Ecuador, Fundación Ecuatoriana Internet Sano y Seguro, Fundación Telefónica Movistar, Instituto Interamericano del Niño, la Niña y Adolescentes. En Consejo Nacional para la Igualdad Intergeneracional, "Política Pública pro una Internet Segura para niños, niñas y adolescentes", septiembre de 2020, 2.

> ofrecen las tecnologías digitales en su vida y su desarrollo, y así, promover el aprovechamiento de los usos y beneficios de las TIC en un marco de derechos (digitales), dignidad e integridad física, psicológica, emocional y sexual.
> Se trata de una política destinada a promover conductas protectoras o preventivas de factores de riesgos que pueden poner en peligro de integridad y dignidad de niñas, niños y adolescentes ante el acceso y uso de internet; y cuando tales vulneraciones han sucedido, promover protocolos adecuados de atención para la protección, atención y reparación.[348]

La política tiene una duración de 10 años, y promovió la creación de la página web https://internetsegura.gob.ec.[349] En esta página se puede encontrar explicaciones sencillas sobre las formas de violencia en Internet y cómo prevenirlas, divididas en secciones con herramientas, consejos, videos y explicaciones dirigidas a padres, educadores y a los propios niños, niñas y adolescentes.[350]

Además de la "Política Pública por una Internet Segura para niñas, niños y adolescentes", no existen más políticas públicas ejecutándose actualmente para salvaguardar específicamente la protección de datos personales de las niñas, niños y adolescentes en Ecuador. Ninguna de las personas entrevistadas indicó conocer políticas públicas en ejecución relacionadas con la salud mental de niños, niñas y adolescentes en el entorno digital.

#### 2.4.4. Subcategoría 4: Instituciones

La Primera Autoridad de Protección de Datos Personales (Superintendente) se posesionó ante el Pleno de la Asamblea Nacional del Ecuador el 23 de abril de 2024.[351] Esta autoridad es quien lidera la Superintendencia de Protección de Datos Personales,[352] institución creada por la LOPDP. De acuerdo con el artículo 213 de la Constitución, "Las superintendencias son organismos técnicos de vigilancia, auditoría, intervención y control de las actividades económicas, sociales y ambientales, y de los servicios que presten las entidades públicas y privadas",[353] esto con el objetivo de que estas actividades se ajusten al ordenamiento jurídico.

Así, la Superintendencia de Protección de Datos del Ecuador tiene la responsabilidad de supervisar, controlar y evaluar el tratamiento de datos personales, con

---

[348] Ibíd., 33-4.

[349] Ibíd., 10.

[350] Godoy, "Internet segura para la niñez y adolescencia", párr. 13.

[351] Fabrizio Peralta-Díaz, "Post de LinkedIn", *Linkedin*, accedido 12 de junio de 2024, https://acortar.link/kSMh7O.

[352] La página web de la Superintendencia de Protección de Datos Personales se encuentra en construcción: https://spdp.gob.ec/

[353] Ecuador, *Constitución de la República del Ecuador*, art. 213.

la potestad de sancionar a responsables, delegados y terceros. Puede resolver reclamos de los titulares, realizar auditorías técnicas, emitir normativas y criterios, y gestionar el Registro Nacional de Protección de Datos. Además, promueve la coordinación internacional, emite autorizaciones para la transferencia internacional de datos, dicta directrices sobre políticas de tratamiento y medidas de seguridad, lleva un registro de vulneraciones, y fomenta la concientización sobre la protección de datos, especialmente para grupos vulnerables como niños, niñas y adolescentes. También tiene competencias en la supervisión del Sistema Nacional de Registros Públicos.[354]

El 19 de agosto de 2024 la Superintendencia publicó su primera resolución, mediante la cual se aprobó el Estatuto Orgánico de Gestión Organizacional donde se establece la estructura y los proceso de la Institución.[355] El 10 de septiembre de 2024 la Superintendencia publicó la Guía Técnica obligatoria para el registro de los apoderados especiales de responsables extranjeros que realicen actividades de tratamiento de datos personales en el Ecuador,[356] y en octubre de 2024, desde su cuenta oficial de *Linkedin* se presentó al equipo de arranque de datos de la Superintendencia.[357]

La Superintendencia de Protección de Datos Personales, aunque recién establecida, ha demostrado un avance significativo en la implementación de la normativa sobre protección de datos en Ecuador. Con la posesión de su primera autoridad en abril de 2024, y las primeras resoluciones y guías técnicas publicadas en pocos meses, queda claro que, aunque esta institución es nueva, está tomando medidas firmes para regular el tratamiento de datos personales en el país. A través de su labor, la Superintendencia se perfila como un actor clave para garantizar la protección de derechos en un entorno digital

---

[354] Ecuador, *Ley Orgánica de Protección de Datos Personales*, art. 76.

[355] La Superintendencia de Protección de Datos personales publicó en el Tercer Suplemento del Registro Oficial No. 624 el 19 de agosto de 2024 el Estatuto Orgánico de Gestión Organizacional por procesos de Arranque. Este documento detalla la misión, estructura y direccionamiento institucional de la entidad. Esta resolución también se otorga un plazo de 180 días desde el 02 de agosto de 2024 para que la Dirección Administrativa Financiera presente a las instancias competentes la demanda de servicios y productos de la Superintendencia para su aprobación. En Arianna Sáenz, "Post de LinkedIn", *Linkedin*, accedido 23 de agosto de 2024, https://www.linkedin.com/feed/update/urn:li:activity:7231455505955651584/.

[356] El Segundo Suplemento del Registro Oficial 640, publicado el 10 de septiembre de 2024, contiene la guía técnica obligatoria para el registro de los apoderados especiales de responsables y encargados extranjeros que realizan tratamiento de datos personales en Ecuador. Esta guía cumple con lo establecido en el artículo 3 del Reglamento General de la Ley Orgánica de Protección de Datos Personales. En ella se dispone que los apoderados designados no pueden tener limitaciones o condiciones que afecten los derechos de los titulares de los datos. Esta regulación es la primera emitida por la Superintendencia de Protección de Datos Personales, marcando un avance en su labor reguladora. En Fabrizio Peralta-Díaz, "Publicación | LinkedIn", accedido 23 de octubre de 2024, https://acortar.link/lssBeA.

[357] Superintendencia de Protección de Datos Personales, "Superintendencia de Protección de Datos Personales: Publicaciones | LinkedIn", accedido 19 de octubre de 2024, https://acortar.link/mRigQI

cada vez más complejo, sentando las bases para una regulación sólida en los próximos años.

### 2.5. Categoría 5: Alternativas

En esta quinta categoría se exploran las alternativas que permitirían reforzar la protección de datos y la salud mental de niños, niñas y adolescentes más allá de la normativa nacional. Se enfatiza la cooperación internacional como mecanismo para contrarrestar el desequilibrio de poder entre Estados y grandes empresas tecnológicas, proponiendo la adhesión a convenios multilaterales (por ejemplo, el Convenio 108+) y la participación activa en redes como la RIPD para habilitar sanciones transfronterizas y homologar estándares de protección.

Al mismo tiempo, se subraya la necesidad de un enfoque integral que vincule la ley con políticas públicas efectivas, estructuras institucionales robustas y una cultura organizacional orientada al cumplimiento. Este enfoque reconoce que la sola existencia de una norma —por más avanzada que sea— no garantiza su aplicación ni su impacto real, por lo que se requiere la articulación de marcos regulatorios, procesos de implementación y educación digital para traducir los derechos formales en prácticas concretas de protección.

#### 2.5.1. Subcategoría 1: Cooperación internacional

Ola Bini, Lorena Naranjo y Santiago Acurio[358] coinciden en que las empresas de datos tienen ventaja frente a muchos estados porque disponen de más recursos que sus gobiernos, que deberían regularlos.[359] Así, resulta complicado regular a entidades más poderosas, incluso si existiera normativa, políticas públicas e instituciones adecuadas, por lo mismo, los entrevistados consideran que la solución debe ser integral, no solo normativa.[360]

En el mismo sentido, expertos consideran que fue un gran error depositar tanta confianza y responsabilidad en las empresas de datos, por lo que sugiere que los gobiernos deben comenzar a utilizar la tecnología para promover sus propios proyectos

[358] Abogado con más de 24 años de experiencia en Derecho Penal e Informático, ex juez de Corte Provincial y exfuncionario de la Fiscalía General del Estado. Es magíster en Derecho Digital y docente universitario, además de autor de libros y artículos sobre delitos informáticos. Ha sido capacitador en cibercrimen para la OEA y miembro fundador de la Asociación Ecuatoriana de Ciberseguridad.

[359] Anexo 4, Ver entrevistas de Bini, Naranjo y Acurio.

[360] Ibíd.

democráticos y no que las empresas tecnológicas los utilicen sólo para lograr sus objetivos.[361]

América Latina no tiene el poder de Europa, que se ha organizado para generar una normativa regional (RGPD) para hacer frente a las grandes empresas de datos, por lo que resulta muy difícil hacer cumplir la normativa nacional a las grandes empresas de datos. No obstante, los entrevistados afirman que se puede tomar su ejemplo, y realizar acciones locales coordinadas entre países para hacer frente a este poder, pues las normas locales no son suficientes.[362] Por lo tanto, urge la cooperación internacional:

> […] cómo el Ecuador podría, por ejemplo, sancionar a *Facebook*, sancionar a *Microsoft*, sancionar a cualquier otro proveedor de servicios de redes sociales. Por eso **necesitamos del tema de Cooperación Internacional y ahí viene justamente el tema del 108 plus**, por lo menos en materia de datos personales […] La autoridad de protección de datos personales en Europa podría sancionar a *Facebook* a *Meta* por un caso que se derivó en el Ecuador, pero siempre y cuando nosotros pertenezcamos o hagamos todo el tema de adecuación a la normativa del 108 plus, que **significaría que el Ecuador sea un puesto seguro para que los datos personales sean almacenados aquí en el Ecuador**.[363]

Ahora bien, ya existen esfuerzos por parte del país para lograr una cooperación internacional. Por ejemplo, el Ecuador, a través de la Autoridad de Protección de Datos Personales, ha quedado oficialmente incorporado a la Red Iberoamericana de Protección de Datos (RIPD), con voz y voto.[364]

La RIPD surgió con motivo del acuerdo alcanzado en el Encuentro Iberoamericano de Protección de Datos celebrado en la Antigua, Guatemala, del 01 al 06 de junio de 2003, con la asistencia de representantes de 14 países iberoamericanos; iniciativa que fue políticamente respaldada a través de la Declaración Final de la XIII Cumbre de Jefes de Estado y de Gobierno de los países iberoamericanos.[365]

En el mismo sentido, Acurio considera que, para garantizar la protección de datos personales de los niños, niñas y adolescentes, Ecuador también debería suscribirse al Convenio 108+.[366] Este convenio es una versión modernizada del Convenio 108, suscrito en 1981 en la ciudad de Estrasburgo-Francia y constituye un instrumento multilateral de

---

[361] DW Documental, "Google, Facebook, Amazon".

[362] Anexo 4, Ver entrevista de Acurio.

[363] Ibíd, El resaltado es propio del autor.

[364] Fabrizio Peralta-Díaz, "Publicación | Feed | LinkedIn", *Linkedin*, accedido 14 de junio de 2024, https://www.linkedin.com/feed/update/urn:li:activity:7204134049756430336/.

[365] "Historia de la Red Iberoamericana de Protección de Datos (RIPD) | Red Iberoamericana de Protección de datos", accedido 14 de junio de 2024, https://www.redipd.org/es/la-red/historia-de-la-red-iberoamericana-de-proteccion-de-datos-ripd.

[366] Anexo 4, Ver entrevista de Acurio, entrevistado por el autor, 11 de junio de 2024.

carácter vinculante en materia de protección de datos personales, que tiene por objeto proteger la privacidad de los individuos contra posibles abusos en el tratamiento de sus datos.[367] En Latinoamérica ha sido suscrito solamente por Uruguay y Argentina.

En conclusión, aunque Ecuador enfrenta desafíos significativos en la regulación y protección de datos personales frente a las grandes empresas tecnológicas, la cooperación internacional y la adhesión a convenios internacionales representan pasos importantes hacia la creación de un marco más robusto y efectivo. La integración en redes como la RIPD y la búsqueda de normativas compartidas a nivel regional pueden fortalecer la capacidad de los países latinoamericanos para proteger los datos de sus ciudadanos y asegurar un uso responsable y equitativo de la tecnología.

### 2.5.2. Subcategoría 2: Enfoque integral

En el abordaje de esta subcategoría, la entrevista con Santiago Acurio resalta que la garantía de derechos como la privacidad de niños, niñas y adolescentes en entornos digitales no puede depender exclusivamente de la existencia de una norma jurídica. Desde su perspectiva, es indispensable un enfoque holístico que articule la normativa con políticas públicas, instituciones responsables, procesos de implementación y cultura organizacional.[368]

Acurio señala que, aunque la Ley de Protección de Datos Personales está vigente desde 2021, muchas empresas aún no cumplen con elementos básicos como registros de actividades de tratamiento o evaluaciones de impacto. En sus palabras: “Solamente con la norma positivizada no solucionas el tema; es como decir, tenemos ley de transformación digital, pero no existe transformación digital en el Estado”.[369] Esta afirmación pone en evidencia la brecha entre la legislación formal y su efectiva implementación, particularmente en lo que respecta a la protección de poblaciones vulnerables como la niñez.

## 3. Análisis de Resultados

El recorrido por las cinco categorías de estudio (impacto en la salud mental, pandemia y virtualidad, corresponsabilidad, protección de datos y alternativas) revela un

[367] Red Iberoamericana de Protección de Datos, “Se convirtió en Ley la aprobación del Convenio 108+ | Red Iberoamericana de Protección de datos”, *Redipd*, 30 de noviembre de 2022, https://www.redipd.org/es/noticias/se-convirtio-en-ley-la-aprobacion-del-convenio-108.

[368] Anexo 4, Ver entrevista de Acurio

[369] Ibíd.

entramado complejo de factores que, en condiciones específicas, potencian riesgos y vulnerabilidades en niños, niñas y adolescentes.

En primer lugar, la sexualización, la ansiedad y la depresión emergen con mayor intensidad cuando el acceso a contenidos digitales no va acompañado de educación crítica ni de controles parentales, condiciones que se agravan en contextos de menor alfabetización digital familiar y escolar. La exposición temprana a pornografía o estándares irreales de belleza propicia rupturas en el desarrollo psicosexual y alimenta comparaciones constantes, que derivan en baja autoestima y trastornos alimentarios. Estas dinámicas cobran fuerza en hogares con brechas de supervisión parental y en entornos sin protocolos de prevención en línea.

El hiperconsumo y la violencia digital funcionan como engranajes de una matriz productiva que explota las inseguridades de las y los adolescentes. Las plataformas incentivan la compra de productos y la viralización de contenido violento, exacerbado cuando faltan sanciones efectivas y rendición de cuentas a las empresas del entorno digital. Estos mecanismos se alimentan de la ausencia de un marco regulatorio que obligue a diseñar entornos digitales seguros y con límites de uso para NNA.

La hiperconectividad y el desplazamiento de la interacción social al espacio virtual fueron impulsados por la pandemia, pero su persistencia pone en evidencia que la tecnología sin acompañamiento psicosocial genera nuevos riesgos: aislamiento afectivo, dependencia de notificaciones y fatiga emocional. En situaciones de confinamiento, la falta de espacios presenciales y la precariedad habitacional (51,2 % en zonas urbanas) intensificaron la vulnerabilidad emocional y el estrés familiar, mostrando la necesidad de reforzar la salud mental comunitaria y programas de contención en línea.

En cuanto a la corresponsabilidad, la familia, el Estado y las empresas digitales actúan de forma fragmentada. Mientras que las familias carecen de alfabetización digital, el Estado no garantiza atención psicológica universal ni educación mediática, y las empresas se rigen por intereses económicos. Esta falta de sinergia explica por qué las leyes vigentes y las políticas públicas (como la “Internet Segura”) no se traducen en prácticas efectivas de protección ni en entornos preventivos para NNA.

En materia de protección de datos, la existencia de un marco jurídico reforzado para NNA (LOPDP, RGPD de referencia) choca con problemas de implementación: la Superintendencia naciente requiere recursos para supervisar, y muchas empresas aún omiten registros de tratamiento y evaluaciones de impacto. La brecha entre norma y

realidad demanda un enfoque integral de responsabilidad administrativa y sancionatoria, así como mayor transparencia sobre la huella digital de los menores.

Finalmente, las alternativas apuntan a la cooperación internacional y a un enfoque integral que combine norma, políticas públicas, educación y cultura organizacional. Solo confrontando la estructura de poder de las empresas de datos con acciones locales coordinadas, alianzas regionales y políticas nacionales de educación digital y salud mental, será posible cerrar las brechas identificadas y atender de manera efectiva las condiciones de riesgo de NNA en el entorno digital.

# Capítulo tercero
# Mecanismos de exigibilidad para garantizar la salud mental de niños, niñas y adolescentes en el entorno digital

> Si crees que la tecnología puede resolver tus problemas de seguridad, entonces no entiendes los problemas y no entiendes la tecnología.
> (Bruce Schneier, 2003)

En este capítulo se señala que, aunque la Constitución ecuatoriana y diversos instrumentos internacionales reconocen el derecho de niños, niñas y adolescentes a la protección de sus datos personales, la creciente digitalización y globalización los expone a un nivel de vulnerabilidad que puede afectar gravemente su salud mental, por lo que ese derecho debe ser activamente exigido mediante una estrategia colectiva. Para ello introduce la exigibilidad estratégica como un proceso social, político y legal que combina la comprensión del adversario, los recursos y el terreno con tácticas coordinadas, y propone el litigio estratégico (que va más allá de reivindicaciones individuales para visibilizar problemas estructurales ante la agenda pública) tomando como caso emblemático la operación de *Worldcoin* en Ecuador, cuyo escaneo de iris plantea riesgos de privacidad y estigmatización de NNA sin un consentimiento libre, informado y específico.

A partir de esa base, el capítulo despliega otras vías de incidencia que, sin enumerarse de forma aislada, convergen en un mismo fin: la garantía efectiva de estos derechos. En el ámbito social se enfatiza la necesidad de campañas de sensibilización en medios y espacios educativos, articuladas con el Ministerio de Educación, universidades y organizaciones civiles, y el diseño de procesos continuos de diagnóstico, talleres, foros y peticiones digitales para mantener la presión más allá de las protestas puntuales; en el político, la activación de los organismos estatales de protección de derechos y los mecanismos de la Asamblea Nacional para fiscalizar a las entidades encargadas de garantizar la protección de éstos; y en el internacional, el recurso a procedimientos especiales de la ONU, al Sistema Interamericano y ejemplos como la prohibición de *Chromebooks* en *Helsingør* (Dinamarca, 2022) bajo el RGPD, para impulsar recomendaciones y sentencias que, al aplicarse directamente en Ecuador, eleven los estándares de protección de datos de niños, niñas y adolescentes.

## 1. Exigibilidad del derecho a la salud mental de niños, niñas y adolescentes en el entorno digital

La protección de los datos personales de niños, niñas y adolescentes es una conquista inscrita en instrumentos internacionales y nacionales, pero la digitalización y la globalización han incrementado la vulnerabilidad de estos grupos frente al entorno digital, lo que puede tener consecuencias adversas para su bienestar mental. Así, el solo reconocimiento de este derecho no implica su garantía, deben ser exigidos.

La exigibilidad estratégica es una institución de los derechos humanos que sirve de herramienta de promoción y protección de éstos.[370] Es un conjunto de decisiones que se toman de acuerdo con los objetivos y metas planteadas, considerando los recursos existentes y el contexto; y citando a Sun Tzu, para su diseño se debe considerar la comprensión del adversario, de nosotros y del terreno.[371]

En el mismo sentido, la Declaración de Quito acerca de la exigibilidad y realización de los Derechos Económicos, Sociales y Culturales menciona que "la exigibilidad es un proceso social, político y legal",[372] por lo que articula diversos mecanismos para impulsar la realización de un derecho.

Por lo tanto, la exigibilidad estratégica en derechos humanos significa elegir tácticas adecuadas que se enmarcan en una estrategia común de diversos actores que cooperan para conseguir lo deseado, relacionando diferentes elementos como la coyuntura local, nacional e internacional, los actores, la institucionalidad y los discursos que se desarrollan a partir del tema de interés.

Las principales vías de exigibilidad identificadas en el capítulo son cuatro, cada una incluida por su papel complementario en una estrategia integral:

1 Vía jurídica: comprende el litigio estratégico (acción de Hábeas Data y trámites administrativos ante la Autoridad de Protección de Datos) que permite visibilizar las violaciones estructurales, generar precedentes vinculantes y ordenar medidas cautelares o sanciones. Se incluye porque a

[370] Mónica Roa y Barbara Klugman, "Considering strategic litigation as an advocacy tool: a case study of the defence of reproductive rights in Colombia", *Reproductive Health Matters* 22, nº 44 (enero de 2014): 31–41, doi:10.1016/S0968-8080(14)44804-3, 117.

[371] Johnson, "La Necesidad de Nuevas Tácticas", 14.

[372] Organizaciones de la Sociedad Civil de Latinoamérica, "Declaración de Quito acerca de la exigibilidad y realización de los derechos económicos, sociales y culturales (DESC) en América Latina y el Caribe", *Derechos*, 24 de julio de 1998, http://www.derechos.org.ve/pw/wp-content/uploads/desc_01.pdf.

través de sentencias y resoluciones formales se puede obligar a las empresas y al Estado a respetar el marco normativo y reforzar la protección de datos de NNA.

2 Vía social: engloba campañas de sensibilización en medios y entornos educativos, conversatorios, talleres y movilizaciones coordinadas que trascienden protestas puntuales. Se fundamenta en que la presión colectiva y el aumento de la conciencia pública son imprescindibles para mantener la agenda viva, empoderar a familias y comunidades, y reforzar la legitimidad de las acciones legales.

3 Vía política: La exigibilidad política es una forma de acción colectiva que busca influir en las decisiones de actores públicos y privados para modificar políticas y garantizar el cumplimiento de los derechos humanos, resolviendo o minimizando conflictos de intereses en la sociedad. Su inclusión responde a que es necesario activar los organismos de derechos humanos y los procesos de fiscalización y control político para garantizar la salud mental de los NNA en el entorno digital.

4 Vía internacional: consiste en recurrir a mecanismos de la ONU (Procedimientos Especiales, Comité de los Derechos del Niño), al Sistema Interamericano (CIDH, Corte IDH), y foros como la Red Iberoamericana de Protección de Datos o convenios supranacionales (ej. Como el Convenio 108+). Se incorpora porque esos instrumentos, directamente aplicables o persuasivos, ofrecen canales adicionales de denuncia, recomendaciones y presión que refuerzan la acción local y exigen al Ecuador elevar sus estándares de protección.

### 1.1. Exigibilidad jurídica

Existen diferentes formas de exigibilidad de derechos humanos que se pueden utilizar para crear una hoja de ruta para enfrentar el presente problema. Entre estos se encuentra la exigibilidad jurídica, expresada en el litigio estratégico, que se caracteriza porque supera el plano individual; es decir, busca el interés público debido a que refleja un problema estructural, por lo que beneficiará a la sociedad y no a individuos.[373] Vale

[373] Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos en México, El litigio estratégico en México: la aplicación de los derechos humanos a nivel práctico: Experiencias de la

aclarar que esta forma de exigibilidad no necesariamente busca una sentencia favorable, sino que se incorpore en la agenda publica un problema social.[374]

Considerando la coyuntura nacional, recientemente fue noticia nacional que la empresa *Worldcoin* se encuentra operando desde finales de junio de 2024 en el Ecuador.[375] Esta empresa escanea el iris de las y los usuarios para "crear una identidad digital única y verificar la humanidad de los participantes, diferenciando entre y humanos y *bots* en la era de la inteligencia artificial".[376]

*Worldcoin* es un proyecto criptográfico fundado por Sam Altman (cofundador de *OpenAI)* junto con Alex Blania y Max Novendstern. Se lanzó oficialmente en 2023 con la idea de crear una red económica global y equitativa mediante la distribución de una criptomoneda, también llamada *Worldcoin*, a todas las personas del mundo.[377]

No obstante, uno de los aspectos más controversiales y discutidos de *Worldcoin* es su método de verificación de identidad. Para garantizar que cada persona solo pueda reclamar su parte de *Worldcoin* una vez, se utiliza un dispositivo llamado *Orb*, que escanea los iris de las personas para crear una identificación única y verificar que no han recibido *Worldcoin* antes.

Este método da lugar a serias preocupaciones sobre la privacidad y el posible mal uso de la información biométrica. De hecho, su actividad ya ha sido cuestionada en 8 países. Por ejemplo, La Agencia Española de Protección de datos, paralizó sus actividades en marzo de 2024, y Argentina los investiga por posibles cláusulas abusivas.[378] Por otro

---

sociedad civil (México, D.F.: Oficina en México del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, 2007), 18.

[374] David Velazco y Rosa Quedena, *La criminalización de la protesta social y el caso Majaz*, (Lima: Fedepaz/Oxfam, 2015), 66.

[375] Esto ha sido objeto de varias noticias. Ver: Pablo Terán, "Una empresa extrae datos de la retina de cientos de ecuatorianos posiblemente violando derechos de privacidad e información personal", *Fundamedios*, 31 de julio de 2024, https://www.fundamedios.org.ec/una-empresa-extrae-datos-de-la-retina-de-cientos-de-ecuatorianos-posiblemente-violando-derechos-de-privacidad-e-informacion-personal/; Lorena Naranjo Godoy, "Los riesgos de entregar datos biométricos personales como el iris", *El Comercio*, 2 de agosto de 2024, https://www.elcomercio.com/?p=1423127; Fundamedios, "30 dólares por escanear tu iris: ¿vale la pena?", *Fundamedios*, accedido 15 de agosto de 2024, https://www.youtube.com/watch?v=UoHqcGYL3Eg; Ecuavisa, El Universo, "Ecuatorianos escanean su iris a cambio de criptomonedas", *Video de YouTube*, 2024, https://www.youtube.com/watch?v=eS4K2SI0TDE.; El Universo, "Cientos permiten escaneo de sus iris por 'bono' en criptomonedas de Worldcoin, en Guayaquil y Quito", 2024, https://www.youtube.com/watch?v=j7Pld5mJ3LU.

[376] Lorena Naranjo Godoy, "Los riesgos de entregar datos biométricos personales como el iris", *El Comercio*, 2, 2 de agosto de 2024, https://www.elcomercio.com/?p=1423127.

[377] Worldcoin, "¡Worldcoin Está En Ecuador!", *Worldcoin*, accedido 15 de agosto de 2024, https://worldcoin.org/holaecuador, 1.

[378] Ecuavisa, "Ecuatorianos escanean su iris a cambio de criptomonedas: Cientos permiten escaneo de sus iris por 'bono' en criptomonedas de Worldcoin", *Ecuavisa*.

lado, el uso de tecnología para capturar datos biométricos de personas en regiones donde la conciencia y comprensión de los riesgos digitales pueden ser limitadas, como el Ecuador, ha generado también críticas éticas.

Con respecto a niños, niñas y adolescentes, se ha denunciado en otros países, como en Chile, México y España, que *Worldcoin* se encuentra recopilando sus datos biométricos a través del escaneo de iris.[379] Esta información genera dudas sobre si están realizando lo mismo en el Ecuador. La recolección de datos biométricos por parte de *Worldcoin* o cualquier otra entidad similar puede tener implicaciones profundas y potencialmente perjudiciales para la salud mental de las y los niños, niñas y adolescentes. Estas implicaciones surgen de una combinación de factores relacionados con la invasión de la privacidad, el desarrollo de la identidad, la explotación de la información personal y el potencial para la discriminación y el estigmatismo.

Los datos biométricos recolectados de niños, niñas y adolescentes pueden ser utilizados, de manera directa o indirecta, para la explotación. En un mundo cada vez más digitalizado, la información personal puede ser manipulada o utilizada en contra de la voluntad del individuo. Por ejemplo, los datos biométricos podrían ser explotados para la vigilancia masiva, la creación de perfiles o la discriminación basada en características físicas. Esta explotación puede tener efectos duraderos en la salud mental de un niño, niña o adolescente, incluyendo el desarrollo de problemas de confianza, miedo a la tecnología, y un sentimiento constante de vulnerabilidad.[380]

Además, si estos datos son utilizados para clasificar o estigmatizar a los niños, niñas y adolescentes (por ejemplo, en contextos escolares o comunitarios), esto puede llevar al desarrollo de sentimientos de inferioridad o marginación. El estigma asociado con ciertas características biométricas, especialmente si son compartidas con terceros o

---

[379] Nativa Digital, "La Amenaza Silenciosa del Escaneo de Iris en Niños, niñas y adolescentes", *Nativa Digital*, accedido 15 de agosto de 2024, https://nativadigital.org/la-amenaza-silenciosa-del-escaneo-de-iris-en-niños, niñas y adolescentes/; Renato Coronel Altamirano, "Worldcoin: Autenticación de Humanos vs. Protección de Datos Personales", *GVN Abogados*, 14 de marzo de 2024, https://gvn.com.ec/2024/03/14/worldcoin-autenticacion-de-humanos-vs-proteccion-de-datos-personales/,11; C. N. N. Chile, "Corte Admite Recurso Contra Empresa Internacional Por Escaneo Del Iris a Menor de Edad a Cambio de Criptomonedas", *CNN Chile*, accedido 15 de agosto de 2024, https://www.cnnchile.com/pais/corte-recurso-proteccion-menor-de-edad-datos-biometricos-iris-criptomonedas_20240325/; elEconomista, "Worldcoin, la polémica empresa que escaneaba el iris de niños, niñas y adolescentes por criptomonedas cesa su actividad en España", *elEconomista*, 4 de junio de 2024, https://www.eleconomista.es/actualidad/noticias/12848184/06/24/worldcoin-la-polemica-empresa-que-escaneaba-el-iris-de-niños, niñas y adolescentes-por-criptomonedas-cesa-su-actividad-en-espana.html; Anna Lagos, "Worldcoin llega a México y establece una economía paralela a cambio de datos personales", *WIRED*, 29 de mayo de 2024, 46, https://es.wired.com/articulos/worldcoin-llega-a-mexico-y-establece-una-economia-paralela-a-cambio-de-datos-personales.

[380] Anexo 4, ver entrevista de Salao y Zaruma.

mal gestionadas, puede llevar a una disminución en la autoestima y un aumento en los trastornos de ansiedad y depresión.[381]

La Autoridad de Protección de Datos ya se ha pronunciado con respecto a *Worldcoin*. Así, hace un llamado a la ciudadanía para que "en ejercicio de una libertad responsable, exijan siempre, con firmeza, su derecho a recabar de los responsables o encargados toda la información que les permita conocer, con claridad y precisión, cuáles serán los fines y los tipos de tratamiento que se harán de sus datos…"[382]

Esto considerando que los datos biométricos, como el iris, son datos objeto de especial regulación y protección al constituirse como datos sensibles, toda vez que sirven para identificar o individualizar a las personas. Así, está prohibido el tratamiento de este tipo de datos, salvo que el titular del derecho haya dado su consentimiento explícito.[383] Sin embargo, este consentimiento es válido solo si es libre, específico, informado e inequívoco.[384]

Lorena Naranjo, entrevistada, también ha comentado sobre esta empresa, señalando que no se sabe dónde *Worldcoin* almacena la información. Además, se pregunta:

> ¿Cómo sabemos que en el futuro no cambiará de opinión sobre el uso de esa información? No hay forma para monitorear los usos posteriores. Solo pensemos lo que pasa con *Facebook.* Se suponía que nuestras fotos y mensajes solo servían para que nos comuniquemos, pero el 26 de junio enviaron un comunicado en el que informan que van a alimentar con eso la inteligencia artificial.[385]

De esta manera, alerta a las personas que no existe garantía que en lo posterior la empresa pueda cambiar el uso sobre el tratamiento de los datos sin consentimiento de sus titulares.

Patricia,[386] usuaria de *Worldcoin*[387] señala que no conoce para qué utilizará *Worldcoin* sus datos biométricos, y que se registró porque le comentaron sus compañeros del trabajo que le iban a pagar 8 dólares en criptomonedas por escanearle el iris. También menciona que no le hicieron firmar ningún documento:

---

[381] Ibíd.

[382] Fabrizio Peralta-Díaz, "Post de LinkedIn", *Linkedin*, 7 de agosto de 2024, https://www.linkedin.com/feed/update/urn:li:activity:7226964273808248832/.

[383] Ecuador, *Ley Orgánica de Protección de Datos Personales*, art. 26.a.

[384] Ibíd., art. 8.

[385] Naranjo Godoy, "Los riesgos de entregar datos biométricos personales como el iris", 27.

[386] Seudónimo para garantizar el anonimato.

[387] Usuaria de Worldcoin, entrevistada el 17 de agosto de 2024; ver Anexo 4.

> Ingresé, ajá, te toman los datos, te dan una explicación muy breve que solamente te dicen detallado que es un registro único. Que va a ser como una huella digital, pero a través del iris. Y más nada, pasas como a una cámara y colocas tu retina, más nada, o sea, el ojo […] **no sé qué va a pasar, o sea, no sé de qué trata, no sé con qué fin**. Ahora sí, yo digo, pero quizá la necesidad te hace ciego.[388]

Es notorio que actualmente existe interés en el presente tema, lo que puede servir para posicionar el litigio estratégico para garantizar la salud mental de los niños, niñas y adolescentes a través de la protección de sus datos personales. Así, el litigio estratégico consistiría en visibilizar y judicializar la recolección masiva de datos biométricos de niños, niñas y adolescentes sin un consentimiento libre, informado y específico, fundamentado en la Constitución, la LOPDP y los estándares internacionales de derechos de la niñez y adolescencia; sus objetivos serían lograr pronunciamientos que declaren estas prácticas ilegales, ordenen salvaguardias y sienten precedentes vinculantes, así como presionar para el fortalecimiento normativo y regulatorio. Para ello se aportaría con testimonios, informes psicológicos sobre el impacto en la salud mental, estudios técnicos y testimonios de familias, se articularían alianzas con organizaciones de infancia y derechos digitales y se utilizaría una estrategia de comunicación (campañas mediáticas, ruedas de prensa y foros públicos). El avance del litigio se puede medir mediante indicadores como cambios normativos, sanciones impuestas y cobertura mediática, buscando al final una sentencia con efectos generales, resoluciones administrativas vinculantes y la promoción de proyectos de ley y directrices de buenas prácticas para proteger la privacidad y la salud mental de las y los NNA en Ecuador.

Ahora bien, aunque el caso de *Worldcoin* no involucra directamente el uso del entorno digital, su inclusión en este informe de investigación es fundamental para ilustrar la amplitud y complejidad del desafío que enfrentan los derechos de niños, niñas y adolescentes en el contexto digital contemporáneo, específicamente en lo que respecta a la protección de sus datos personales y el impacto en su salud mental.

*Worldcoin* ofrece un ejemplo emblemático de cómo las empresas pueden utilizar incentivos económicos para recolectar datos biométricos extremadamente sensibles, incluyendo los de niños, niñas y adolescentes, sin un adecuado consentimiento informado ni salvaguardias que protejan su integridad y bienestar. Este caso es relevante porque pone de manifiesto la creciente tendencia de las corporaciones de extraer datos de usuarios y usuarias vulnerables, una práctica que, aunque en este caso no esté ligada directamente

[388] Anexo 4, Ver entrevista de “Patricia”.

con el entorno digital, sigue estando dentro del mismo paradigma de explotación de datos personales que se ha demostrado perjudicial para la salud mental y el bienestar general de los niños, niñas y adolescentes.

El uso de este caso para incidir jurídicamente permite posicionar la protección de datos personales como un tema central en la defensa del derecho a la salud mental. El modelo de negocio de *Worldcoin,* basado en la recolección masiva de datos biométricos establece un precedente peligroso que podría ser extrapolado a otras plataformas digitales, incluidas las redes sociales. Esta conexión es crucial, ya que la salud mental de NNA puede verse comprometida tanto por la explotación de sus datos en el entorno digital como por la recolección indiscriminada de datos biométricos. Ambas prácticas comparten un denominador común: la explotación de datos personales sin la debida protección y consideración de los efectos sobre el bienestar de los individuos, especialmente de las y los niños, niñas y adolescentes.

Además, abordar el caso de *Worldcoin* en este contexto tiene un valor estratégico para el avance de la protección de datos personales en el Ecuador.[389] Al posicionar este caso como un ejemplo de vulneración de derechos, se establece una base sólida para demandar una mayor regulación y supervisión de todas las formas de recolección y procesamiento de datos personales, incluyendo los realizados en el entorno digital. De esta manera, se fortalece el argumento de que la protección de datos personales es una pieza clave para garantizar el derecho a la salud de los niños, niñas y adolescentes, independientemente de la plataforma o medio en el que esos datos sean recolectados.

A continuación, se plantean dos vías para realizar litigio estratégico (constitucional y la administrativa) que podrían proponerse a través de organizaciones de derechos de la niñez y adolescencia como Grupo Rescate Escolar y/o la Junta Metropolitana de Protección de Derechos de la Niñez y Adolescencia de Quito, con organizaciones de derechos humanos con experiencia en litigio, como el Centro de Derechos Humanos de la Pontificia Universidad Católica del Ecuador.

### 1.1.1. Vía administrativa

[389] El 5 de noviembre de 2024 la Superintendencia de Protección de Datos Personales informa sobre el inicio de investigaciones administrativas en una institución pública y en una empresa privada del sector tecnológico (Worldcoin) por presuntas vulneraciones a la seguridad de datos personales y al tratamiento de datos sensibles. En Superintendencia de Protección de Datos Personales, "Post de LinkedIn", *LinkedIn*, 5 de noviembre de 2024, https://acortar.link/pId4vh.

La LOPDP concibe en su décimo capítulo que el titular podrá en cualquier momento, de forma gratuita y por medios físicos o digitales presentar "requerimientos, peticiones, quejas o reclamaciones directamente al responsable del tratamiento".[390] Estas deben estar relacionadas con el ejercicio de sus derechos, la aplicación de principios y el cumplimiento de obligaciones por parte del responsable del tratamiento, mismo que debe contestar y ejecutar lo que corresponda en el término de 10 días.[391]

Así, se puede requerir a *Worldcoin,* como responsable del tratamiento, que informe sobre la finalidad y el tratamiento de los datos biométricos que ha obtenido de NNA, así como las medidas de protección que ha implementado para garantizar la privacidad de sus usuarios, conforme lo ordena la LOPDP.

Si el responsable del tratamiento no responde al requerimiento dentro del plazo estipulado en la LOPDP, o si la respuesta es negativa, el titular tiene la opción de presentar un reclamo administrativo ante la Autoridad de Protección de Datos Personales. Este reclamo deberá seguir el procedimiento establecido en el Código Orgánico Administrativo, así como las disposiciones de la LOPDP y las normativas emitidas por la Autoridad de Protección de Datos Personales.[392]

La Autoridad de Protección de Datos Personales, ya sea de oficio o a solicitud del titular, también puede llevar a cabo acciones preliminares con el objetivo de investigar las circunstancias del caso en cuestión o evaluar la conveniencia de iniciar el procedimiento, que se regirá por lo dispuesto en el Código Orgánico Administrativo.[393]

La Autoridad de Protección de Datos Personales puede dictar medidas correctivas en caso de que se observe el incumplimiento de sus regulaciones emitidas, de la LOPD, y/o de su reglamento. Estas medidas pueden implicar el cese del tratamiento, la eliminación de los datos y la imposición de medidas para garantizar un tratamiento adecuado de datos personales, entre otras.[394]

De acuerdo con la LOPDP, es una infracción leve no tramitar a tiempo o negar sin justificación los requerimientos realizados por el titular, así como no disponer políticas de protección de datos personales.[395] Son infracciones graves el utilizar datos para fines distintos a los declarados, o no implementar medidas para garantizar que el tratamiento

---

[390] Ecuador, *Ley Orgánica de Protección de Datos Personales*, art. 62.
[391] Ibíd.
[392] Ibíd., art.64.
[393] Ibíd., art. 63.
[394] Ibíd., art. 65.
[395] Ibíd., art. 67.

de datos personales se realice conforme a la LOPDP, su reglamento y las regulaciones emitidas por la Autoridad de Datos Personales.[396]

Por infracciones leves, la Autoridad de Protección de Datos Personales puede imponer a la empresa una multa que varíe entre el 0,1 % y el 0,7 % de su volumen de negocio,[397] basado en el ejercicio económico inmediatamente anterior a la imposición de la sanción.[398] En caso de infracciones graves, la multa puede oscilar entre el 0,7 % y el 1 % de su volumen de negocio, calculado igualmente sobre el ejercicio económico previo a la imposición de la sanción.[399]

La imposición de sanciones económicas por parte de la Autoridad de Protección de Datos Personales constituye un mecanismo crucial para garantizar el cumplimiento de la LOPDP. Estas sanciones no solo buscan penalizar a las empresas que incumplen con las normativas, sino también fomentar una cultura de responsabilidad y transparencia en el manejo de los datos personales.

Además, la posibilidad de imponer multas proporcionales al volumen de negocio de las empresas infractoras introduce un elemento disuasivo importante, promoviendo el cumplimiento de las obligaciones legales y la protección de datos personales. Sin embargo, más allá de las sanciones monetarias, lo verdaderamente importante y lo que se busca en este tipo de litigio estratégico es asegurar que las normas se cumplan de manera efectiva.

El objetivo final no es únicamente castigar las infracciones, sino garantizar que las empresas y los responsables del tratamiento de datos adopten prácticas que respeten y protejan los derechos de los individuos, contribuyendo así a la construcción de un entorno digital seguro. La eficacia de este tipo de litigio radica en su capacidad para crear precedentes legales, incidir en las personas y obligar a las instituciones a cumplir con sus mandatos, asegurando que la LOPDP se implemente de manera integral y efectiva.

### 1.1.2. Vía constitucional

La institución del Hábeas Data, introducida en el país por primera vez en la reforma constitucional de 1996, nace en la época moderna con el desarrollo de la

[396] Ibíd., art. 68.

[397] El artículo 73 de la LOPDP indica que "se entiende por volumen de negocio, a la cuantía de la venta de productos y de la prestación de servicios realizados por operadores económicos, durante el último ejercicio que corresponda a sus actividades, previa deducción del Impuesto al Valor Agregado y de otros impuestos directamente relacionados con la operación económica". Ibíd., art. 73.

[398] Ibíd., art. 71.

[399] Ibíd., art. 72.

informática y las nuevas tecnologías de comunicación, como una respuesta a las nuevas posibilidades de archivo, difusión y acceso a información.[400]

La Constitución ecuatoriana reconoce esta figura en el artículo 92, y menciona que toda persona tiene derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, personales y/o informes que se tengan de esta o sobre sus bienes que consten en entidades públicas o privadas.

Asimismo, esta institución garantiza el derecho a conocer el uso que se ha haga de ellos, su finalidad, el origen y destino de la información y el tiempo de vigencia del banco de datos, pudiendo solicitar su actualización, rectificación, eliminación o anulación. Además, se establece que la ley o la persona titular debe autorizar el archivo de los datos sensibles, y que se debe exigir la adopción de las medidas de seguridad necesarias.[401] La LOGJCC en su artículo 49 menciona lo mismo, pero agregando en su último inciso que la reparación integral debe incluir obligaciones materiales e inmateriales.[402] Por lo tanto, el fin de esta acción no es meramente procesal, sino que sirve para proteger de manera prioritaria los derechos de los NNA frente al tratamiento inadecuado de su información, garantizando su salud mental, su desarrollo integral y su privacidad.

Esta acción se puede interponer luego de que se haya negado el acceso o la eliminación, rectificación o actualización de los datos personales,[403] por lo que es necesario realizar una solicitud previa a la empresa, en la que se puede requerir que informe sobre la finalidad y el tratamiento de los datos biométricos que ha obtenido, así como las medidas de protección que ha implementado para garantizar la privacidad de NNA. Esta solicitud debe seguir las normas del Código Orgánico Administrativo.

Esta garantía jurisdiccional se puede interponer en conjunto con una medida cautelar, "con el objeto de evitar o hacer cesar la violación o amenaza de violación de un derecho",[404] por lo que se puede solicitar que se suspenda de inmediato el escaneo biométrico de NNA hasta resolver el fondo del asunto.[405] De igual manera, pueden

---

[400] Rosa Elena De la Torre y Juan Montaña Pinto, "El habeas data en Ecuador", en *Apuntes de derecho procesal constitucional*, t. 2 (Quito: CEDEC, 2012), 179.

[401] Ecuador, Constitución de la República del Ecuador, art. 92.

[402] Ecuador, Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, art. 49.

[403] Ibíd., art. 50.

[404] Ecuador, Constitución de la República del Ecuador, art. 87.

[405] De acuerdo con el segundo inciso del artículo 26 de la LOGJCC, estas medidas podrían incluir la suspensión provisional de las actividades de la empresa, al menos hasta que se conozca el fondo de la causa.

sumarse *Amicus Curiae* de organizaciones de niñez y adolescencia conforme al artículo 12 de la LOGJCC.[406]

Además, de acuerdo con el artículo 18 de la LOGJCC y el tercer numeral del artículo 86 de la Constitución, en caso de constatarse la vulneración de derechos fundamentales al interponer una garantía jurisdiccional (como lo es el Hábeas Data), la jueza o juez debe ordenar la reparación integral por el daño material e inmaterial.[407]

Entre las medidas que se pueden solicitar como reparación integral se encuentran la investigación y sanción de los responsables por la violación de derechos, así como medidas que garanticen la no repetición, como la implementación de políticas diferenciales de protección de datos para NNA, y actos públicos de reconocimiento de responsabilidad. Con esto se busca no solo el control del flujo de información, sino un verdadero resguardo del bienestar psicológico y los derechos fundamentales de los NNA.[408]

### 1.2. Exigibilidad social

La exigibilidad social, entendida como la capacidad de las personas para demandar el cumplimiento de sus derechos y ejercer presión sobre las instituciones públicas y privadas,[409] es fundamental en un entorno donde los derechos digitales se ven cada vez más amenazados por la recolección y explotación indiscriminada de datos personales.

La protección de datos personales de niños, niñas y adolescentes en Ecuador es ante todo un problema colectivo que, sin embargo, enfrenta la complejidad de que muchas vulneraciones aún no se visibilizan ni se asumen como causa común. La exigibilidad social, por tanto, no se agota en protestas o marchas; implica también articular alianzas entre organizaciones no gubernamentales, movimientos sociales, instituciones educativas y medios de comunicación para, por ejemplo, promover una campaña conjunta que obligue al Ministerio de Educación a incorporar protocolos de privacidad biométrica en

---

[406] Ecuador, Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, art. 12.

[407] Ecuador, Constitución de la República del Ecuador, art. 86.3; Ecuador, Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, art. 18.

[408] También se puede solicitar a la Defensoría del Pueblo que patrocine la acción, o en todo caso, que vigile el debido proceso en la tramitación de la causa. En Ecuador, Constitución de la República del Ecuador, art. 215.1.4.

[409] GKA Comunicación, "Exigibilidad de los derechos", Vídeo de YouTube, 2014, https://www.youtube.com/watch?v=N0oPTSns8tQ.; Mario Melo Cevallos y Justicia y Sociedad, Sarayaku ante el sistema interamericano de derechos humanos: Justicia para el pueblo del medio día y su selva viviente (Bogotá Centro de Estudios de Derecho Colombia), 2016, 61.

las escuelas o impulsar un foro público donde padres de familia, expertos en derechos digitales y representantes de la Defensoría del Pueblo acuerden un plan de acción que presione a los legisladores a regular el uso de tecnología de escaneo de iris en los espacios comunitarios. De ese modo, la exigibilidad social se convierte en un entramado de actividades coordinadas (cartas públicas, talleres, peticiones digitales y espacios de diálogo) que colectivizan el reclamo y aseguran una respuesta integral al riesgo que enfrentan las y los menores.

Las alianzas son cruciales para asegurar que las demandas de la ciudadanía sean escuchadas y atendidas por quienes tienen el poder de implementar cambios; por ello, una hoja de ruta de exigibilidad social podría comenzar por mapear y articular espacios colectivos (como foros escolares, Juntas Cantonales de Protección de Derechos de la Niñez y Adolescencia, plataformas digitales comunitarias, alianzas con escuelas, colegios y facultades de psicología de universidades) y vincularlos con organizaciones aliadas, por ejemplo *World Vision*, UNICEF, *Children International* y la Red Nacional de Niñas, Niños, Adolescentes y Jóvenes *Wamprakunapak Yuyaykuna*. A continuación, se podrían establecer etapas: (1) diagnóstico compartido de vulneraciones en entornos digitales; (2) diseño de campañas de sensibilización conjuntas (talleres, *webinars* y cartas públicas) impulsadas por las ONGs; (3) lanzamiento de peticiones digitales y recogida de firmas en colegios y comunidades; (4) realización de foros multiparticipativos con representantes de la Defensoría del Pueblo y la Asamblea Nacional; y (5) seguimiento y evaluación de compromisos legislativos y administrativos obtenidos. De este modo, la exigibilidad social trasciende el acto individual de reclamo y se convierte en un proceso colectivo, estratégico y continuo para proteger a los más vulnerables en el entorno digital.

Es crucial comprender que los niños, niñas y adolescentes no son simplemente usuarios pasivos de la tecnología, sino que son activos participantes en el entorno digital. Sin embargo, su participación en este espacio viene acompañada de riesgos significativos, incluyendo la explotación de sus datos personales por parte de empresas tecnológicas que buscan monetizar cada interacción digital. En este contexto, la exigibilidad social se convierte en una herramienta clave para proteger a esta población.

La protección de los datos personales no es solo una cuestión de privacidad; es también una cuestión de salud mental y bienestar general, especialmente para los niños, niñas y adolescentes. Los datos personales, cuando son utilizados sin el consentimiento informado o son manipulados para influir en las decisiones y comportamientos de los individuos, pueden tener consecuencias devastadoras para la salud mental de NNA.

A nivel nacional existe poco conocimiento de esta problemática, lo que explica que pese a la existencia de normativas que regulan este fenómeno, aún no se garantiza la protección de datos personales en el Ecuador, ni se lo articula con la salud mental de los NNA, razón por la cual, una empresa como *Worldcoin* se encuentra operando actualmente en el país extrayendo información sensible de sus usuarios, que han manifestado no haber sido informados sobre el fin del tratamiento de sus datos personales.

Por otro lado, en Ecuador, la autoridad encargada de la protección de datos personales necesita ser fortalecida para que pueda cumplir eficazmente su rol. Esto incluye dotarla de mayores recursos y autonomía para supervisar y hacer cumplir la normativa de manera efectiva. Una institución fuerte y autónoma es esencial para que la exigibilidad social tenga un impacto real. Sin una autoridad reguladora capaz de actuar con independencia y recursos adecuados, cualquier esfuerzo por parte de la ciudadanía para exigir el cumplimiento de sus derechos puede quedar en la nada. Por eso, parte de la exigibilidad social debe incluir la presión para que se fortalezca esta institución, asegurando que tenga las capacidades necesarias para proteger los datos personales de los niños, niñas y adolescentes. Así, se proponen las siguientes estrategias de incidencia social para posicionar en la agenda pública la protección de los datos personales de niños, niñas y adolescentes:

### 1.2.1. Campañas de sensibilización en redes y medios

Las campañas de sensibilización deben extenderse más allá de los canales digitales y tradicionales para incidir directamente en el ámbito educativo. Por ejemplo, se puede colaborar con el Ministerio de Educación para incluir módulos sobre protección de datos y salud mental digital en el currículo escolar, formando a docentes en talleres presenciales y virtuales, y diseñando guías didácticas que se distribuyan en unidades educativas. Al mismo tiempo, en redes sociales y medios de comunicación, estas campañas pueden apoyarse en la voz de expertos, alianzas con *influencers*[410] y testimonios de la academia (investigadores y catedráticos de universidades nacionales) que validen la información con datos empíricos.

Se pueden organizar ruedas de prensa y desayunos de trabajo tanto con periodistas como con representantes del Ministerio de Educación, así como *webinars* y foros académicos abiertos a padres de familia y estudiantes, donde se presente el caso de litigio

[410] Este enfoque de pares es especialmente efectivo, ya que los niños, niñas y adolescentes tienden a estar más receptivos a los mensajes que provienen de sus propios grupos de referencia

estratégico contra *Worldcoin* y sus implicaciones para la salud mental de NNA. Para maximizar el alcance, es clave diseñar materiales accesibles y atractivos (infografías, videos cortos, presentaciones interactivas) con el apoyo de comunicadores especializados, y evaluar periódicamente el impacto de la intervención mediante encuestas en colegios y estudios académicos piloto que midan cambios en el nivel de conciencia y en las prácticas de protección de datos.

### 1.2.2. Conversatorios y talleres

Es fundamental que las instituciones educativas asuman un rol activo en la protección de los derechos digitales de los estudiantes. Las escuelas y universidades no solo deben incorporar en sus currículos contenidos sobre derechos digitales y ciberseguridad, sino que también deben servir como espacios donde los niños, niñas y adolescentes puedan organizarse y movilizarse para exigir la protección de sus derechos. Esto no solo educa a los niños, niñas y adolescentes sobre sus derechos, sino que también los empodera para que se conviertan en agentes activos en la protección de estos derechos.

Los conversatorios son espacios clave para el diálogo y la reflexión sobre la protección de datos personales. Estos eventos, que se podrían planificar con las diferentes universidades del país, permiten reunir a expertos en ciberseguridad, activistas de derechos digitales, educadores y miembros de la comunidad para debatir y profundizar en la comprensión de las políticas actuales y las medidas necesarias para mejorar la protección de datos.

Asimismo, se pueden planificar talleres de capacitación sobre protección de datos personales, de uso saludable de redes sociales, y prevención de riesgos en la red con escuelas y colegios, dirigidos tanto a padres de familia como a niños, niñas y adolescentes, con el propósito de concientizar sobre este fenómeno, para que identifiquen los riesgos y tomen acción para exigir al Estado y a las empresas de datos que garanticen su protección en el entorno digital. Estos eventos pueden ser retransmitidos en redes sociales para maximizar su alcance.

### 1.2.3. Movilizaciones, plantones y marchas

Las movilizaciones, plantones y marchas son acciones colectivas de gran visibilidad que se pueden utilizar para exigir un entorno digital saludable, pero en el Ecuador operan en un escenario complejo: muchas protestas nacen de violaciones de derechos en las que el Estado es parte (por ejemplo, en el caso de los cuatro niños de las

Malvinas, asesinados por militares), y con frecuencia pierden fuerza al cabo de días o semanas. Por ello, al convocar marchas en torno al caso de *Worldcoin* o jornadas de protesta vinculadas a la salud mental digital, es clave reconocer esas dinámicas (la desconfianza hacia las instituciones y la temporalidad de la movilización) y articularlas con organizaciones de ciberseguridad y de defensa de la niñez y adolescencia, para que la exigibilidad social no se reduzca a un acto puntual. Estas iniciativas deben anunciarse previamente a medios y redes, llevarse a cabo en fechas estratégicas (por ejemplo, coincidiendo con audiencias, con el Día Internacional de la Protección de Datos o con el Día Mundial de la Salud Mental), e incluir la distribución de volantes educativos que informen a la ciudadanía sobre sus derechos y las vías de acción legal y administrativa.

### 1.2.4. Colaboración con actores internacionales y nacionales

Para fortalecer la estrategia de exigibilidad social, es fundamental articular alianzas con agencias internacionales y locales que aporten experiencia técnica, recursos y legitimidad. UNICEF Ecuador podría colaborar facilitando líneas de base sobre la protección de datos de NNA, diseñando guías didácticas para escuelas y capacitando a docentes del Ministerio de Educación en protocolos de salud mental en el entorno digital; además podría apoyar la implementación de comités escolares de vigilancia de datos y financiar talleres de resiliencia psicosocial ante riesgos digitales. *Children International* y *Save the Children* podrían aportar redes de trabajo con comunidades vulnerables y acciones de seguimiento regional, mientras que organizaciones de salud mental locales, como la Asociación Ecuatoriana de Psicólogos, pueden brindar asistencia técnica para evaluar y mitigar los impactos de la salud mental en el entorno digital de NNA.

En el ámbito de la protección de datos, entidades como *Privacy International*,[411] Derechos Digitales[412] y la Asociación para el Progreso de las Comunicaciones (APC)[413] pueden realizar metodologías de auditoría de bases de datos y herramientas de incidencia

[411] Privacy International busca proteger la democracia, defender la dignidad de las personas y exigir la rendición de cuentas de las instituciones que violan la confianza pública. En Article 29 Data Protection Working Party, "Privacy International | About Privacy International", accedido 9 de noviembre de 2021, https://www.privacyinternational.org/about.

[412] Derechos Digitales es una organización de alcance latinoamericano, independiente y sin fines de lucro, fundada en 2005 y que tiene como objetivo fundamental el desarrollo, la defensa y la promoción de los derechos humanos en el entorno digital. El trabajo de la organización se concentra en tres ejes fundamentales, libertad de expresión, privacidad y datos personales y derechos de autor y acceso al conocimiento. "Derechos Digitales".

[413] Association for Progressive Communications es una red mundial que apoya el uso de Internet y las TICs para la justicia social y el desarrollo sostenible."APC (@APC_News) / Twitter", *Twitter*, accedido 9 de noviembre de 2021, https://twitter.com/APC_News.

legal, y servirían de puente para internacionalizar el debate, invitando a mecanismos de la ONU y grupos de derechos digitales a pronunciarse. Por su parte, el Centro de Autonomía Digital (CAD), al tener su sede en el país podría mapear plataformas y proyectos (como *Worldcoin*) que recolectan datos biométricos en el país, evaluando riesgos de privacidad y elaborando informes técnicos para el litigio estratégico. Con este entramado de actores locales e internacionales la campaña ganaría fuerza para presionar por regulaciones específicas, protocolos diferenciados para NNA y protocolos de monitoreo y sanción efectivos en el Ecuador.

Así, la salud mental NNA en el entorno digital es un desafío complejo que requiere de la colaboración de todos los sectores de la sociedad. Solo a través de una exigibilidad social robusta, colectiva e inclusiva se podrán generar los cambios necesarios para asegurar que los derechos digitales de niños, niñas y adolescentes sean respetados y protegidos en el Ecuador. Este enfoque integral y sostenible es fundamental para enfrentar los desafíos del entorno digital y construir una sociedad donde los derechos de los más vulnerables sean garantizados y protegidos.

### 1.3. Exigibilidad política

La exigibilidad política es un tipo de acción colectiva orientada a influir en las instituciones públicas y privadas para modificar sus políticas, lo que implica administrar el poder con la intención de resolver o minimizar los conflictos de intereses dentro de una sociedad.[414] Así, la exigibilidad política se refiere al uso de estrategias y acciones que buscan influir en las decisiones de los actores políticos y en la formulación de políticas públicas, con el fin de garantizar el cumplimiento de los derechos humanos.

En el presente caso, se plantea este tipo de exigibilidad con el propósito de que las autoridades y actores relevantes adopten políticas efectivas que aseguren que la salud mental en el entorno digital de los niños, niñas y adolescentes sean protegida adecuadamente. Ahora bien, es necesario considerar que en febrero de 2025 en el Ecuador se elegirá al nuevo presidente o presidenta y a nuevos asambleístas, por lo que es crucial aprovechar el período electoral para incidir en la inclusión del derecho a la salud mental de niños niñas y adolescentes en el entorno digital en las agendas de los candidatos y partidos políticos. Así, se proponen las siguientes incidencias de carácter político:

[414] Toda exigibilidad de derechos humanos conlleva elementos políticos, ya que cualquier forma de incidencia busca generar un cambio para garantizar su protección, lo cual implica, inevitablemente, adoptar una posición política. Instituto Interamericano de Derechos Humanos, Inclusión, derechos humanos e incidencia política (San José, Costa Rica: Inst. Interamericano de Derechos Humanos, 2004), 31.

### 1.3.1. Activar a las instituciones de derechos humanos

Es fundamental presionar que instituciones como la Defensoría del Pueblo y la Subsecretaría de Derechos Humanos[415] se involucren activamente en este proceso, considerando que ambas instituciones tienen como mandato la protección de derechos humanos.[416]

Para ello, se pueden solicitar reuniones con los representantes de estas instituciones para discutir la importancia de proteger los datos personales y su impacto en los derechos humanos, buscando de esta manera que se emitan comunicados conjuntos que respalden la causa. Asimismo, se pueden organizar campañas públicas para exigir que estas instituciones prioricen la protección a los datos personales, especialmente de niños, niñas y adolescentes.

### 1.3.2. Crear y fortalecer redes para activar los procesos de fiscalización y control político

Es esencial fortalecer redes ciudadanas dedicadas a la protección del derecho a la salud mental en el entorno digital de niños, niñas y adolescentes, con el fin de lograr una incidencia efectiva tanto en instituciones privadas como públicas. Estas redes pueden coordinar diversas acciones, como enviar cartas abiertas a empresas de datos como *Worldcoin*, *Meta*, *Google*, *TikTok*, entre otras, exigiendo transparencia en sus políticas de manejo de datos. De igual manera, es posible dirigir cartas a los gobiernos de los países donde estas compañías tienen su sede, solicitando regulaciones más estrictas para proteger los datos personales a nivel global, especialmente para niños, niñas y adolescentes.

Por otro lado, la Ley Orgánica de la Función Legislativa (LOFL) dedica un capítulo completo a la fiscalización y el control político, señalando que estas actividades son responsabilidad de las y los asambleístas, las comisiones especializadas y al Pleno de la Asamblea Nacional".[417] Esta herramienta puede utilizarse para garantizar el cumplimiento de las normativas existentes, promover la creación de nuevas regulaciones

[415] Secretaría adjunta al Ministerio de la Mujer y Derechos Humanos.

[416] Ecuador, *Constitución de la República del Ecuador*, Registro Oficial 449, 20 de octubre de 2008, art. 215.; Ministerio de la Mujer y Derechos Humanos, "Subsecretaría de Derechos Humanos", Ministerio de la Mujer y Derechos Humanos, 6 de noviembre de 2019, https://www.derechoshumanos.gob.ec/subsecretaria-de-derechos-humanos-ec/, 1.

[417] Ecuador, Ley Orgánica de la Función Legislativa, art.74.

que fortalezcan la protección del derecho a la salud mental de NNA en el entorno digital o exigir explicaciones y responsabilidades en casos de vulneraciones de derechos.

Por eso es importante establecer vínculos estratégicos con las y los asambleístas o las comisiones legislativas, ya que tienen la capacidad de fiscalizar, lo que permite asegurar que las instituciones públicas cumplan con la LOPDP. Con respecto a las instituciones privadas, los asambleístas pueden requerir a la entidad pública encargada de regularlos, como la Superintendencia de Protección de Datos Personales, que requiera información a la institución privada. Si se detectan irregularidades pueden solicitar comparecencias en la Asamblea Nacional a los funcionarios públicos para esclarecer los hechos.[418] La falta de comparecencia o la entrega de información incompleta podría ser motivo de un juicio político.[419]

Así, la combinación de presión política, activismo social, creación de redes y el uso de la coyuntura electoral puede resultar en un impulso significativo para que la protección de datos personales se convierta en una prioridad en las agendas políticas en Ecuador. La participación activa de la sociedad civil y el aprovechamiento del momento electoral son claves para lograr un cambio sustancial en este campo.

### 1.4. Exigibilidad internacional

La protección de datos personales de los niños, niñas y adolescentes requiere una perspectiva internacional debido a la naturaleza global de las tecnologías de la información y la comunicación. El Derecho Internacional de los Derechos Humanos ha evolucionado desde un enfoque destinado únicamente a regular las relaciones entre Estados, hacia uno en el que estos aceptan gradualmente limitar su soberanía y reconocer la participación de otros actores internacionales, como las organizaciones internacionales[420] y la sociedad civil.[421]

A través de la incidencia internacional, individuos, comunidades, organizaciones y Estados pueden exigir la prevención y detención de las violaciones, así como la implementación de medidas correctivas. Esto impulsa a gobiernos y empresas a asumir su responsabilidad, activando mecanismos para sancionar a los responsables, investigar

[418] Ibíd., arts. 75-6.
[419] Ibíd., art. 76.
[420] Como la OIT, FAO, UNESCO, OMS, etc.
[421] Carlos Villán Durán, Manual sobre el sistema universal de protección de los derechos humanos, 2016, https://www.aepdiri.org/index.php/las-publicaciones/libros-de-los-miembros/589-c-villan-duran-manual-sobre-el-sistema-universal-de-proteccion-de-los-derechos-humanos, 15.

las violaciones de derechos, reparar a las víctimas y garantizar que las normas internacionales se apliquen de manera efectiva.

Un ejemplo ilustrativo de este tipo de acción ocurrió en 2022 en la ciudad de Helsingør, Dinamarca. En ese caso, la autoridad nacional de protección de datos determinó que el municipio no había evaluado adecuadamente los riesgos del uso de tecnologías educativas de *Google* (como los *Chromebooks* y el *software* escolar), lo que comprometía la privacidad de aproximadamente 8,000 estudiantes. Como consecuencia, se prohibió el uso de estos productos en las escuelas. Esta decisión, basada en el Reglamento General de Protección de Datos europeo(GDPR), tuvo un fuerte impacto nacional e internacional al poner en el centro del debate la necesidad de garantizar la privacidad de los menores frente a grandes empresas tecnológicas.[422]

Así, se puede aplicar la exigibilidad internacional para aprovechar los mecanismos que ofrece con el propósito de denunciar las vulneraciones del derecho a la salud mental de NNA en el entorno digital. En Ecuador es especialmente útil, pues su constitución manifiesta que se deben aplicar directamente las normas previstas en los instrumentos internacionales de derechos humanos cuando son más favorables a las establecidas a nivel nacional;[423] e incluso señala una acción específica para garantizar la aplicación de sentencias o informes de organismos internacionales de derechos humanos.[424]

Se plantean las siguientes incidencias de carácter internacional para garantizar la protección de los datos personales de los niños, niñas y adolescentes en Ecuador:

### 1.4.1. Incidencia a través del Sistema Universal de Protección de Derechos Humanos Internacionales

La presión internacional puede ser determinante a la hora de exigir la garantía de derechos. Se puede denunciar las violaciones de derechos a través de los Procedimientos Especiales del Consejo de Derechos Humanos, los órganos de tratados de derechos humanos o en el Consejo de Derechos Humanos:

#### 1.4.1.1. Procedimientos especiales

[422] Morgan Meaker, "A Danish City Built Google Into Its Schools—Then Banned It", Wired, accedido 5 de mayo de 2025, https://www.wired.com/story/denmark-google-schools-data/.

[423] Ecuador, *Constitución de la República del Ecuador*, Registro Oficial 449, 20 de octubre de 2008, art 426.

[424] La Acción por Incumplimiento. Ibíd., Art 93.

Los mecanismos de Procedimientos Especiales, también llamado procedimiento público de quejas individuales

> engloba a órganos especiales de investigación que tienen distinta denominación y mandatos relativamente diversos…pueden dedicar su atención a la situación de todos los derechos humanos en un país o área regional concreta (procedimientos geográficos, actualmente son 14), o bien a un tema específico (desapariciones, ejecuciones, tortura, detención arbitraria, etc.) en todos los Estados Miembros de las Naciones Unidas en los que esa cuestión tenga una gravedad consistente (procedimientos temáticos: actualmente son 46).[425]

Estos procedimientos pueden interactuar directamente con Estados y actores no estatales, como empresas y organizaciones intergubernamentales, en relación con violaciones de derechos humanos dentro de sus mandatos, mediante el intercambio de cartas y comunicaciones sobre presuntas violaciones del derecho a la salud mental de niños, niñas y adolescentes en el entorno digital.[426]

Las denuncias pueden ser presentadas por individuos, grupos, comunidades, organizaciones de la sociedad civil o entidades nacionales de derechos humanos (como la Defensoría del Pueblo). Cada experto decide si tomar acción sobre una denuncia en función de la información disponible y su mandato específico, sin que sea necesario agotar previamente los recursos internos.[427]

Así, para denunciar violaciones al derecho a la protección de datos personales y el derecho a la salud mental de niños, niñas y adolescentes en entornos digitales, se puede recurrir a los siguientes Procedimientos Especiales de las Naciones Unidas:

- Relator Especial sobre el derecho a la privacidad:[428] este procedimiento es clave para denunciar violaciones al derecho a la protección de datos personales, incluyendo el mal manejo de información personal y datos sensibles, especialmente cuando afecta a niños, niñas y adolescentes.[429]

---

[425] Villán Durán, *Manual sobre el sistema universal de protección de los derechos humanos,* 103.

[426] Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, "Notificación de violaciones", *OHCHR*, accedido 16 de septiembre de 2024, párr. 7, https://www.ohchr.org/es/reporting_violations.

[427] Ibíd.

[428] Mandato establecido por Resolución del Consejo de Derechos Humanos A/HRC/RES/55/3. En Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, "Special Procedures Thematic mandates", accedido 17 de septiembre de 2024, https://spinternet.ohchr.org/ViewAllCountryMandates.aspx?Type=TM&lang=sp.

[429] Este punto también resulta clave para que Ecuador retome sus compromisos establecidos en EPU sobre estas materias.

- Relator Especial sobre el derecho de toda persona al disfrute del más alto nivel posible de salud física y mental:[430] Este mandato se enfoca en el derecho a la salud, incluyendo la salud mental de niños, niñas y adolescentes, y puede abordar casos relacionados con entornos digitales que afecten negativamente su bienestar.
- Relatora Especial sobre la violencia contra las mujeres y las niñas, sus causas y consecuencias:[431] esta relatora puede abordar situaciones donde los entornos digitales afecten el bienestar y seguridad de las niñas, incluyendo la protección de sus datos y su salud mental.
- Grupo de Trabajo sobre la cuestión de los derechos humanos y las empresas transnacionales y otras empresas:[432] dado que muchas violaciones de derechos en el entorno digital involucran a empresas tecnológicas, este procedimiento es relevante para denunciar el rol de estas compañías en la protección insuficiente de datos y sus efectos en la salud mental de los niños, niñas y adolescentes.
- Relator Especial sobre el derecho a la educación:[433] este relator puede abordar cuestiones relacionadas con el acceso y el impacto de la educación en entornos digitales, así como la necesidad de educar a los niños, niñas y adolescentes en la protección de datos personales.

Se pueden realizar comunicaciones utilizando la herramienta de envío en línea y solicitar su visita al país. Estas acciones pueden servir para obtener intervención internacional, presión sobre los Estados, las empresas y visibilidad internacional, con el propósito de generar cambios en políticas que pueden resultar en la corrección de violaciones y mejoras estructurales en la protección de los derechos a la salud mental en entornos digitales y a la protección de datos personales.

#### 1.4.1.2. Sistema de Tratados

[430] Mandato establecido por Resolución del Consejo de Derechos Humanos A/HRC/RES/51/21. Ibíd.

[431] Mandato establecido por Resolución del Consejo de Derechos Humanos A/HRC/RES/50/7. Ibíd.

[432] Mandato establecido por Resolución del Consejo de Derechos Humanos A/HRC/RES/53/3. Ibíd.

[433] Mandato establecido por Resolución del Consejo de Derechos Humanos A/HRC/RES/53/7. Ibíd.

Los tratados de derechos humanos son acuerdos internacionales que, una vez ratificados, crean obligaciones jurídicas para los Estados de proteger, promover y garantizar los derechos y libertades que en ellos se establecen.[434] El Ecuador ha ratificado los nueve tratados de derechos humanos de Naciones Unidas.[435] Cada uno de estos tratados crea un comité compuesto por expertos independientes, cuya responsabilidad es supervisar de diversas maneras el cumplimiento de las disposiciones establecidas en éstos.[436]

Todos estos órganos, excepto el Subcomité para la Prevención de la Tortura, tienen el mandato de recibir y examinar informes periódicos de los Estados parte, en los que se detalla cómo se aplican las disposiciones de los tratados. Estos comités emiten observaciones generales sobre la interpretación de estas disposiciones, y la mayoría también puede examinar denuncias o comunicaciones de individuos que aleguen violaciones de sus derechos por parte de un Estado, siempre que dicho Estado haya reconocido este procedimiento.[437]

Así, se puede recurrir a los siguientes comités de expertos independientes de Naciones Unidas para presionar el buen cumplimiento de la protección de datos personales y la salud mental de niños, niñas y adolescentes en el entorno digital:

- Comité de los derechos del Niño: compuesto por 18 miembros y establecido en 1991 para supervisar la aplicación de la Convención sobre los Derechos del Niño, así como sus dos protocolos facultativos (sobre conflictos armados y la venta de niños, niñas y adolescentes, prostitución infantil y la utilización de niños, niñas y adolescentes en la pornografía).[438]

---

[434] Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, "Notificación de violaciones", 6.

[435] Convención Internacional sobre la Eliminación de Todas las Formas de Discriminación Racial (1965); Pacto Internacional de Derechos Civiles y Políticos (1966); Convención sobre la Eliminación de Todas las formas de Discriminación contra la Mujer 1979); Convención contra la Tortura y Otros Tratos o Penas Crueles, Inhumanos o Degradantes (1984); Convención sobre los Derechos del Niño (1989); Convención Internacional sobre la Protección de los Derechos de Todos los Trabajadores Migratorios y de sus Familiares (1990); Convención sobre los Derechos de las Personas con Discapacidad (2006); y la Convención Internacional para la Protección de Todas las Personas contra las Desapariciones Forzadas (2006).

[436] Oficina del Alto Comisionado de Naciones Unidas, *El sistema de tratados de derechos humanos de las Naciones Unidas*, Folleto informativo Nro. 30/Rev. 1 (Nueva York y Ginebra, 2012), 22, https://www.ohchr.org/Documents/Publications/FactSheet30Rev1_sp.pdf.

[437] Ibíd., 24.

[438] Ibíd., 23.

Esta convención garantiza los derechos de los niños, niñas y adolescentes, incluyendo el derecho a la salud[439] y a la no injerencia arbitraria o ilegal en sus vidas privadas,[440] así como a la protección contra todas las formas de explotación, abuso y tratamiento negligente,[441] lo que podría incluir la protección de los datos y la salud mental en el entorno digital.

- Comité de Derechos Humanos: se creó en 1976 y cuenta con 18 miembros para examinar la aplicación del Pacto Internacional de Derechos Civiles y Políticos.[442]

  Esta convención incluye derechos relacionados con la privacidad, fundamentales parala protección de datos personales. También protege contra injerencias arbitrarias en la vida privada de las personas, un aspecto crucial en el contexto digital.[443]

- Comité de Derechos Económicos, Sociales y Culturales: se creó en 1985 para vigilar el cumplimiento del Pacto Internacional de Derechos Económicos, Sociales y Culturales. Se compone por 18 miembros.[444]

  Este pacto protege el derecho al más alto nivel posible de salud, lo que incluye la salud mental.[445] También protege los derechos de los niños, niñas y adolescentes y el acceso a la educación, que puede verse afectado por el entorno digital.[446]

- Comité para la eliminación de la discriminación contra la mujer: Integrado por 23 miembros, revisa la aplicación de la Convención sobre la eliminación de todas las formas de discriminación contra la mujer desde 1981.[447]

  En esta convención hay varios artículos que, interpretados desde un enfoque de derechos digitales y protección de la salud mental, pueden servir para

---

[439] ONU Asamblea General, "Convención sobre los Derechos del Niño", 20 de diciembre de 1989, Resolución 44/25, art. 24.

[440] Ibíd., art. 16.

[441] Ibíd., art. 19, 36.

[442] Oficina del Alto Comisionado de Naciones Unidas, *El sistema de tratados de derechos humanos de las Naciones Unidas,* 22.

[443] ONU Asamblea General, "Pacto Internacional de Derechos Civiles y Políticos", 16 de diciembre de 1966, Resolución 2200A (XXI), art. 17.

[444] Oficina del Alto Comisionado de Naciones Unidas, *El sistema de tratados de derechos humanos de las Naciones Unidas*, 22.

[445] ONU Asamblea General, "Pacto Internacional de Derechos Económicos, Sociales y Culturales", 16 de diciembre de 1966, art. 12.

[446] Ibíd., art.13.

[447] Oficina del Alto Comisionado de Naciones Unidas, *El sistema de tratados de derechos humanos de las Naciones Unidas*, 23.

> abordar la situación de las niñas y adolescentes en el entorno digital, tales como la obligación de eliminar la discriminación digital,[448] protección de la salud mental,[449] o el acceso igualitario a la educación digital segura.[450]

En todos estos mecanismos se pueden solicitar la emisión de observaciones generales para que aclaren cómo los tratados internacionales aplican específicamente a la protección de datos y la salud mental en entornos digitales. También se puede participar en los informes periódicos que el Estado debe rendir a los comités, enviando informes paralelos que aporten a una perspectiva alternativa. Asimismo, se puede solicitar su intervención (una vez que se hayan agotado todos los recursos nacionales) a través de comunicaciones individuales y requerir que emitan recomendaciones específicas al Estado para mejorar su marco normativo y de políticas públicas para asegurar que se respete el derecho a la protección de datos personales y la salud mental de niños, niñas y adolescentes en entornos digitales.

#### 1.4.1.3. Consejo de Derechos Humanos

El Consejo de Derechos Humanos, creado en 2006 por la Asamblea General para reemplazar a la antigua Comisión de Derechos Humanos, es el principal órgano intergubernamental de las Naciones Unidas[451] encargado de

> promover el respeto universal de la protección de todos los derechos humanos y libertades fundamentales de todas las personas… (de) estudiar las situaciones de infracciones graves y sistemáticas de los derechos humanos, así como hacer recomendaciones al respecto y promover la coordinación eficaz y la incorporación de los derechos humanos en la actividad general del sistema de las Naciones Unidas[452]

El Consejo, compuesto por 47 Estados miembros de las Naciones Unidas, constituye un foro multilateral para abordar las violaciones de los derechos humanos y la situación de los países. Responde a las emergencias de derechos humanos y hace

---

[448] A través del artículo 2 (obligación de eliminar la discriminación) y 5 (estereotipos de género y violencia). En ONU Asamblea General, "Convención sobre Eliminación de toda Discriminación contra la Mujer", 18 de octubre de 1979.

[449] A través del artículo 12, para garantizar que el Estado implemente medidas de protección de la salud mental en entornos digitales, especialmente para niñas y adolescentes. Ibíd.

[450] El artículo 10 puede servir para exigir que las niñas tengan acceso una educación en línea que no ponga en riesgo su privacidad y bienestar psicológico. Ibíd.

[451] Oficina del Alto Comisionado de Naciones Unidas, "Acerca del CDH", *OHCHR*, accedido 20 de septiembre de 2024, párr. 3, https://www.ohchr.org/es/hr-bodies/hrc/about-council.

[452] Villán Durán, *Manual sobre el sistema universal de protección de los derechos humanos,* 134.

recomendaciones sobre cómo aplicar mejor los derechos humanos sobre el terreno. El Consejo cuenta con el apoyo sustantivo, técnico y de secretaría de la Oficina del Alto Comisionado para los Derechos Humanos (OACDH).[453]

En este marco, se puede aprovechar el Examen Periódico Universal (EPU),[454] que implica una revisión hecha al Ecuador por sus pares de su historial de derechos humanos cada cuatro años y medio.[455] Así, las organizaciones de la sociedad civil pueden presentar informes paralelos, que serán considerados en el proceso de evaluación del país.[456] Se puede presentar un informe que destaque violaciones o lagunas en la protección de los datos personales y la salud mental de niñas, niños y adolescentes en entornos digitales en el país.

De momento no es posible utilizar el procedimiento de denuncia del Consejo de Derechos Humanos debido a que para esto es necesario haber agotado los recursos de la jurisdicción interna primero.[457]

### 1.4.2. Incidencia a través del Sistema Interamericano de Protección de Derechos Humanos

El Sistema Interamericano de Protección de los Derechos Humanos (SIDH) es el mecanismo regional encargado de la promoción y protección de los derechos humanos en América. A través de la Organización de Estados Americanos (OEA), los países de la región han adoptado varios instrumentos internacionales que fundamentan este sistema. El SIDH establece y reconoce los derechos humanos, imponiendo responsabilidades a los Estados para su cumplimiento y protección, además de crear órganos encargados de

[453] Oficina del Alto Comisionado de Naciones Unidas, "Acerca del CDH", párrs. 4-5.

[454] De acuerdo con Villán Durán, el EPU no promueve eficazmente los derechos humanos entre los Estados miembros, sino que debilita el sistema de protección de los derechos humanos, debido a que considera que el Estado interesado "se verá tentado a prestar más atención a las recomendaciones políticas que le han puesto sus pares en el seno del EPU y que ha aceptado voluntariamente, que a cumplir sus obligaciones jurídicas de dar cumplimiento a las recomendaciones emanadas de los órganos de protección que han sido habilitados al efecto por el DIDH". En Villán Durán, *Manual sobre el sistema universal de protección de los derechos humanos*, 141.

[455] La última revisión del Ecuador fue en 2022; Oficina del Alto Comisionado de Naciones Unidas, "Mecanismos y entidades del Consejo de Derechos Humanos", *OHCHR*, accedido 20 de septiembre de 2024, párr. 3, https://www.ohchr.org/es/hr-bodies/hrc/other-sub-bodies.

[456] "4th UPR Cycle: Contributions and Participation of 'Other Stakeholders' in the UPR", *OHCHR*, accedido 20 de septiembre de 2024, párr. 2, https://www.ohchr.org/en/hr-bodies/upr/ngos-nhris.

[457] Villán Durán, *Manual sobre el sistema universal de protección de los derechos humanos*, 143.

supervisar su respeto, como la Comisión Interamericana de Derechos Humanos y la Corte Interamericana de Derechos Humanos.[458]

#### 1.4.2.1. Comisión Interamericana de Derechos Humanos (CIDH)

La CIDH es un órgano principal y autónomo de la OEA, cuyo mandato de promoción y protección de los derechos humanos en el continente americano surge de la Carta de la OEA y de la Convención Americana sobre Derechos Humanos. Actúa en representación de todos los países miembros de la OEA y está integrada por siete miembros independientes elegidos por la Asamblea General de la OEA, que se desempeñan en forma personal (no representan a ningún país en particular). Tiene su sede en Washington, D.C.[459]

La CIDH realiza su trabajo con base en tres pilares, el sistema de Petición Individual; el monitoreo de la situación de los derechos humanos en los Estados Miembros; y la atención a líneas temáticas prioritarias.[460] Así, se pueden activar los siguientes mecanismos dentro de la CIDH:

- Relatorías:

A partir de 1990, la Comisión Interamericana comenzó a establecer Relatorías Temáticas con el propósito de enfocar su atención en grupos, comunidades y pueblos que, debido a su vulnerabilidad y a la discriminación histórica que han sufrido, están especialmente expuestos a violaciones de derechos humanos. El objetivo de estas Relatorías es fortalecer, promover y organizar de manera más sistemática el trabajo de la Comisión en esos temas específicos.[461]

Así, se puede acudir a la Relatoría sobre los Derechos de la Niñez[462] para abordar los riesgos que enfrentan los niños, niñas y adolescentes en el entorno digital, como la

---

[458] Manuel Ventura Robles, "El Sistema Interamericano de Protección de los Derechos Humanos", en *Los sistemas internacionales de protección de los derechos humanos*, 1.ª ed. (Universidad del Externado de Colombia, 2014), doi: 10.2307/j.ctv13vdg3r, 257.

[459] Comisión Interamericana de Derechos Humanos, "¿Qué es la CIDH?", *Comisión Interamericana de Derechos Humanos (CIDH)*, accedido 20 de septiembre de 2024, párr. 1, https://www.oas.org/es/CIDH/jsForm/?File=/es/cidh/mandato/que.asp.

[460] Ibíd.

[461] OEA, "Relatorías y Unidades Temáticas", Text, accedido 27 de septiembre de 2024, párr. 1, https://www.oas.org/es/CIDH/mandato/relatorias.asp.

[462] Creada en 1998 con el fin de fortalecer el respeto de los derechos humanos de los niños, niñas y adolescentes en las Américas. La Relatoría está a cargo de un Comisionado o Comisionada nombrada por el pleno de la Comisión. Esta Relatoría asesora a la CIDH en el trámite de peticiones, casos y solicitudes de medidas cautelares y provisionales en materia de niñez y adolescencia. También realiza visitas a los Estados y elabora estudios e informes. En OEA, "CIDH: Relatoría sobre los Derechos de la Niñez", *Comisión Interamericana de Derechos Humanos (CIDH)*, accedido 27 de septiembre de 2024, párrs.1-2, https://www.oas.org/es/CIDH/jsForm/?File=/es/cidh/r/DN/default.asp.

vulneración de su privacidad, el mal manejo de sus datos personales y las consecuencias negativas en su salud mental.

También se puede acudir a la Relatoría sobre los Derechos de las Mujeres[463] con el fin de informar sobre las situaciones de riesgo desproporcionada a las que se enfrentan las niñas y adolescentes en el entorno digital, como la falta de control sobre sus datos personales, lo que conlleva al deterioro de su salud mental.

Por último, se puede recurrir a la Relatoría Especial sobre los Derechos Económicos, Sociales, Culturales y Ambientales[464] considerando que se enfoca en derechos relacionados con la salud y educación, para trabajar en el impacto que el entorno digital tiene en la salud mental de niñas, niños y adolescentes con relación al uso de plataformas digitales y redes sociales.

Acudiendo a estas relatorías se pueden obtener informes temáticos, recomendaciones al Estado ecuatoriano y medidas de protección que garanticen tanto la protección de datos personales como la salud mental de niñas, niños y adolescentes en entornos digitales.

- Audiencias

Desde 2022 la CIDH lleva a cabo tres sesiones anuales,[465] durante las cuales escucha a la sociedad civil y organiza encuentros entre representantes de los Estados y la sociedad para discutir los desafíos relacionados con los derechos humanos en la región.[466]

Las audiencias tienen como objetivo recopilar información sobre la situación de los derechos humanos en relación con temas específicos o asuntos en determinados países

---

[463] La Relatoría sobre los Derechos de las Mujeres, creada en 1994, presta atención específica a los derechos humanos de las mujeres y la equidad e igualdad de género. Esta Relatoría formula recomendaciones para el cumplimiento por parte de los Estados de sus obligaciones prioritarias de igualdad y no discriminación, prepara estudios especializados e informes, asiste a la Comisión en la respuesta a peticiones y demás informes de violaciones de estos derechos en la región OEA, "CIDH: Relatoría sobre los Derechos de las Mujeres", *Comisión Interamericana de Derechos Humanos (CIDH)*, accedido 27 de septiembre de 2024, párrs. 2-3, https://www.oas.org/es/CIDH/jsForm/?File=/es/cidh/r/DMUJERES/default.asp.

[464] Creada en 2017, esta Relatoría representa un esfuerzo por especializar y profundizar en la promoción y protección de los Derechos Económicos, sociales, culturales y ambientales en el ámbito del trabajo de la CIDH, y es un reconocimiento de la importancia de estos derechos para la realización de la dignidad en un contexto de crecientes desafíos globales y regionales OEA, "CIDH: Relatoría Especial sobre los Derechos Económicos, Sociales, Culturales y Ambientales", *Comisión Interamericana de Derechos Humanos (CIDH)*, accedido 27 de septiembre de 2024, párr. 10, https://www.oas.org/es/CIDH/jsForm/?File=/es/cidh/r/DESCA/default.asp.

[465] Comisión Interamericana de Derechos Humanos, "CIDH: Sesiones", *Comisión Interamericana de Derechos Humanos (CIDH)*, accedido 27 de septiembre de 2024, https://www.oas.org/es/cidh/sesiones/default.asp.

[466] Comisión Interamericana de Derechos Humanos, "Períodos de Sesiones", *Canal CIDH*, accedido 27 de septiembre de 2024, https://www.canalcidh.org/periodos-de-sesiones.

o en la región, y emitir recomendaciones para promover el respeto y disfrute de esos derechos.[467]

Así, se puede solicitar una audiencia temática para el siguiente período de sesiones, sobre la protección de datos personales y el derecho a la salud mental de niños, niñas y adolescentes en entornos digitales, con el objetivo de que la CIDH se informe y emita recomendaciones al Ecuador para que garantice estos derechos en el país.

#### 1.4.2.2. Corte Interamericana de Derechos Humanos (CorteIDH)

La Corte Interamericana es uno de los tres tribunales regionales dedicados a la protección de los derechos humanos, junto con la Corte Europea de Derechos Humanos y la Corte Africana de Derechos Humanos y de los Pueblos. Es un organismo judicial independiente cuya misión es aplicar e interpretar la Convención Americana sobre Derechos Humanos (CADH).[468] La Corte cumple una función contenciosa,[469] que incluye la resolución de casos y el monitoreo del cumplimiento de sentencias;[470] además, tiene una función consultiva[471] y la facultad de dictar medidas provisionales.[472]

Así, se puede presionar desde la exigibilidad social y política al Estado para que active la función consultiva, considerando que a través de este mecanismo la CorteIDH responde a consultas presentadas por los Estados miembros de la OEA (como el Ecuador),

---

[467] Comisión Interamericana de Derechos Humanos, "CIDH: Información sobre audiencias", *Comisión Interamericana de Derechos Humanos (CIDH)*, accedido 27 de septiembre de 2024, párr. 1, https://www.oas.org/es/CIDH/jsForm/?File=/es/cidh/sesiones/coberturas.asp.

[468] Corte Interamericana de Derechos Humanos, "ABC de la Corte Interamericana de Derechos Humanos", 2018, 6, https://repositorio.consejodecomunicacion.gob.ec/bitstream/CONSEJO_REP/1138/1/ABCCorteIDH.pdf.

[469] De acuerdo con el artículo 35 del Reglamento de la CorteIDH, el caso debe ser sometido por parte de la CIDH, conteniendo "todos los hechos supuestamente violatorios, inclusive la identificación de las presuntas víctimas". En Corte Interamericana de Derechos Humanos, "Reglamento de la Corte Interamericana de Derechos Humanos", noviembre de 2009, art. 35, https://www.corteidh.or.cr/sitios/reglamento/nov_2009_esp.pdf.

[470] De acuerdo con el artículo 69 del Reglamento de la CorteIDH, la supervisión de las sentencias y demás decisiones de la Corte se realizará mediante "la presentación de informes estatales y de las correspondientes observaciones a dichos informes por parte de las víctimas o sus representantes". Asimismo, cuando lo considere pertinente, el "Tribunal podrá convocar al Estado y a los representantes de las víctimas a una audiencia para supervisar el cumplimiento de sus decisiones" .En Ibíd., art. 69.1.69.3.

[471] De acuerdo con el artículo 70 del Reglamento de la CorteIDH, las solicitudes de opinión consultiva deben "formular con precisión las preguntas específicas sobre las cuales se pretende obtener la opinión de la Corte". Si la solicitud es formulada por un Estado miembro, debe indicar, además de las disposiciones cuya interpretación se pide, las consideraciones que originan la consulta y el nombre y dirección del Agente o de los Delegados; y si la iniciativa de la opinión consultiva es de otro órgano de la OEA distinto de la Comisión, debe precisar también la manera en que la consulta se refiere a su esfera de competencia. Ibíd., art. 70.1.2.3.

[472] De acuerdo con el artículo 27 del Reglamento de la CorteIDH, cuando se trate de "casos de extrema gravedad y urgencia y cuando sea necesario para evitar daños irreparables a las personas, la Corte, de oficio, podrá ordenar las medidas provisionales que considere pertinentes, en los términos del artículo 63.2 de la Convención". Ibíd., art. 27.1.

sobre la compatibilidad de las leyes internas con la CADH y sobre la interpretación de la CADH o de otros tratados relacionados con la protección de los derechos humanos en los Estados Americanos.[473]

De esta manera, se puede solicitar a la CorteIDH que se pronuncie sobre la compatibilidad de la LOPDP y de su reglamento con la CADH, así como sobre la interpretación de la CADH con relación a la protección de datos personales y el derecho a la salud mental de niños, niñas y adolescentes en entornos digitales.

### 1.4.3. Otros instrumentos internacionales

Existen instrumentos e instancias internacionales fuera del Sistema Interamericano y del Sistema Universal de derechos humanos que también son útiles para ejercer presión internacional:

#### 1.4.3.1. Red Iberoamericana de Protección de Datos (RIPD)

La Red Iberoamericana de Protección de Datos (RIPD) se creó como resultado de un acuerdo alcanzado durante el Encuentro Iberoamericano de Protección de Datos, celebrado en La Antigua, Guatemala, del 1 al 6 de junio de 2003, con la participación de representantes de 14 países iberoamericanos.[474]

De acuerdo con su reglamento, la RIPD busca fomentar la cooperación en protección de datos, promover políticas y tecnologías para garantizar este derecho, ofrecer asistencia técnica, establecer acuerdos con instituciones, y participar en foros internacionales, todo con transparencia y capacitación tanto para sus miembros como para las y los ciudadanos.[475]

El Ecuador, a través de la Autoridad de Protección de Datos Personales, es miembro de la Red Iberoamericana de Protección de Datos.[476] Esta instancia realiza el Encuentro Iberoamericano de Protección de Datos, que es un "foro de debate abierto

---

[473] Corte Interamericana de Derechos Humanos, "ABC de la Corte Interamericana de Derechos Humanos", 11.

[474] Red Iberoamericana de Protección de Datos, "Historia de la Red Iberoamericana de Protección de Datos (RIPD)", *REDIPD*, párrs. 1,3 https://www.redipd.org/es/la-red/historia-de-la-red-iberoamericana-de-proteccion-de-datos-ripd.

[475] Red Iberoamericana de Protección de Datos, "Reglamento de la Red Iberoamericana de Protección de Datos", *REDIPD*, 30 de noviembre de 2018, art. 1, https://www.redipd.org/sites/default/files/2019-11/reglamento-ripd.pdf.

[476] Red Iberoamericana de Protección de datos, "Países miembros", s.f., https://www.redipd.org/es/enlaces-de-interes/paises-miembros.; Peralta-Díaz, "Post de LinkedIn"; REDIPD, "Relación de entidades integrantes de la RIPD", accedido 8 de octubre de 2024, https://www.redipd.org/es/la-red/entidades-acreditadas.

sobre las cuestiones relativas a los objetivos de la Red",[477] donde la Autoridad de Protección de Datos Personales del Ecuador puede incidir para exponer sobre la protección de datos personales con relación a la salud mental de los niños y niñas.

Esta red también realiza sesiones cerradas, donde se pueden establecer grupos de trabajo.[478] Así, la Autoridad de Protección de Datos Personales del Ecuador puede solicitar en estas reuniones la creación de un Grupo de Trabajo sobre la protección de datos personales a niños, niñas y adolescentes, con el propósito de que se desarrollen políticas y estrategias específicas para proteger la salud mental de los NNA en el entorno digital.

Este Grupo de Trabajo podría intercambiar buenas prácticas, identificar riesgos emergentes relacionados con la explotación de datos de niños, niñas y adolescentes, y proponer marcos regulatorios y mecanismos de supervisión adecuados. Además, buscaría promover campañas de sensibilización y educación sobre el uso seguro de tecnologías digitales, con el fin de garantizar que los derechos de niños, niñas y adolescentes sean respetados en todo momento en el ámbito digital.[479]

#### 1.4.3.2. Convenio 108+

América Latina no tiene el poder que tiene Europa para enfrentar a las grandes plataformas, pues Europa a través del RGPD logra hacer contrapoder. Por lo tanto, América latina necesita organizarse para promover la ratificación de convenios internacionales que obliguen a los estados y a las empresas a proteger los datos personales de los niños, niñas y adolescentes de edad.

Así, el Convenio 108+, versión moderna del Convenio 108, es una propuesta atractiva para alcanzar estos resultados. El Convenio 108, adoptado por el Consejo de Europa y abierto a la firma de los Estados miembros de la Unión Europea y a la adhesión de los Estados no miembros de la Unión Europea desde 1981, es el primer instrumento internacional vinculante que protege a las personas contra los abusos en la recogida y tratamiento de datos personales, regulando también su flujo transfronterizo. Prohíbe el

[477] Red Iberoamericana de Protección de Datos, "Reglamento de la Red Iberoamericana de Protección de Datos", art. 11.1.

[478] Ibíd., art. 12. c.

[479] De conformidad con el artículo 13 del Reglamento de la RIPD, los Grupos de Trabajo pueden ser temporales o permanentes, desarrollarán un trabajo sistemático y especializado por temas, y estarán conformados por los miembros, observadores, expertos invitados, entidades públicas y organizaciones de la sociedad civil. Ibíd. art. 13.

tratamiento de datos sensibles sin garantías adecuadas y consagra el derecho de las personas a acceder y corregir su información almacenada.[480]

Se modernizó el Convenio 108 en el año 2018 para enfrentar los desafíos que surgen del uso de nuevas tecnologías de la información y la comunicación, y fortalecer la implementación efectiva del Convenio.[481] De esta manera, el Convenio 108+ introduce nuevos derechos para los titulares de datos, actualiza los mecanismos de transferencias internacionales y amplía el concepto de datos sensibles, incluyendo datos genéticos y biométricos. También exige la notificación de incidentes de seguridad, establece requisitos más estrictos para el tratamiento de datos (como proporcionalidad y minimización), impone condiciones especiales para el tratamiento de datos de niños y niñas, y refuerza la obligación de destruir o anonimizar los datos personales.[482]

Ahora bien, en caso de que se firme y ratifique este Convenio, el Ecuador puede solicitar que el Comité del Convenio evalúe si el nivel de protección de datos personales del país se encuentra en cumplimiento con las disposiciones del Convenio, así como solicitar que recomiende las medidas que debería tomar para lograr dicho cumplimiento, conforme se establece en el literal f del artículo 23.[483] También puede solicitar que el Comité examine la implementación del Convenio y que recomiende qué medidas tomar en caso de que el país no cumpliere con el mismo, de acuerdo con el literal h del artículo 23.[484]

En resumen, la ratificación del Convenio 108+ por parte de Ecuador y otros países de América Latina permitiría al país alinearse con los más altos estándares internacionales en protección de datos personales, especialmente en lo referente a niños, niñas y adolescentes en el entorno digital. Esto no solo fortalecería la capacidad del Estado para regular y exigir a las empresas que operan en el país el cumplimiento de estas normativas, sino que también abriría la posibilidad de que el Comité del Convenio monitoree y evalúe la situación en Ecuador, recomendando medidas correctivas cuando sea necesario. De este modo, el Convenio 108+ se convierte en una herramienta clave para garantizar una mayor protección de los datos personales y el bienestar de niños, niñas y adolescentes

[480] Consejo Europeo, "Details of Treaty No.108", párrs. 5-6.

[481] Consejo Europeo, "Modernisation of Convention 108", *Data Protection*, accedido 10 de octubre de 2024, párr. 2, https://www.coe.int/es/web/data-protection/convention108/modernised.

[482] Gobierno de Argentina, "Se convirtió en Ley la aprobación del Convenio 108+", 30 de noviembre de 2022, párr. 5, https://www.redipd.org/es/noticias/se-convirtio-en-ley-la-aprobacion-del-convenio-108.

[483] Consejo Europeo, "Convention 108+", art. 23.f.

[484] Ibíd., art. 23.h.

frente a los riesgos del entorno digital, promoviendo un marco legal más sólido y eficaz en la región.

# Conclusiones

El estudio demuestra con claridad cómo la falta de protección de datos personales en el entorno digital incide directamente en el derecho a la salud mental de niños, niñas y adolescentes en Ecuador, al combinar un análisis profundo de marcos normativos, datos estadísticos nacionales y percepciones de especialistas. La triangulación metodológica reforzó la validez de estos resultados: por un lado, las fuentes secundarias sobre capitalismo de la vigilancia y salud mental digital, junto con el examen de marcos internacionales (RGPD, Convención Americana) y nacionales (LOPDP, LOSM), aportaron el marco teórico necesario para entender tanto la mercantilización de los datos como el marco de protección; por otro, las cinco categorías de estudio (impacto del entorno digital en la salud mental de NNA, pandemia y virtualidad, corresponsabilidad en el entorno digital, protección de datos personales de NNA y alternativas) emergieron de la revisión documental y de las entrevistas semiestructuradas con nueve informantes clave (cuatro psicólogos, cuatro expertos en protección de datos y una usuaria de Worldcoin).

La codificación abierta y axial permitió ordenar estos hallazgos, mientras que la comparación con las obligaciones de la Superintendencia de Protección de Datos confirmó la disparidad entre norma y práctica. Finalmente, las estrategias de exigibilidad (jurídica, social, política e internacional) se definieron a partir de la experiencia de actores nacionales e internacionales, apuntalando propuestas de litigio estratégico, campañas de sensibilización y esquemas de cooperación supranacional.

En el primer capítulo se reveló cómo las plataformas digitales, al basar su modelo de negocio en la recolección masiva de datos y la maximización del tiempo de uso, emplean algoritmos de manipulación (desde la radicalización del pensamiento hasta la exposición continua a contenidos polarizantes y desinformación) que pueden erosionar la autoestima, el equilibrio emocional y la percepción de la realidad de niños, niñas y adolescentes. Casos públicos, como las disculpas de Mark Zuckerberg ante el Senado de EE. UU. por el daño psicológico sufrido por menores en *Instagram* y *Facebook*, o las reconocidas fallas de *Snapchat* en el control de tráfico de drogas, ponen de manifiesto los impactos reales de estas prácticas: sobreestimulación crónica, aislamiento afectivo,

incremento de la ansiedad y la depresión, y exposición a situaciones de ciberacoso y contenidos dañinos.

En Ecuador, la aprobación de la Ley Orgánica de Protección de Datos Personales y de la Ley Orgánica de Salud Mental supone un avance normativo, pero su implementación fragmentada y reactiva deja a los menores en una situación de alta vulnerabilidad. La desconexión entre estándares internacionales (que ya integran un enfoque preventivo, interseccional y estructural de la salud mental digital) y el marco nacional, anclado en lógicas adultocéntricas y carente de protocolos específicos para NNA, impide abordar de forma integral la relación entre protección de datos y bienestar psicológico. Para cerrar estas brechas, resulta imprescindible reformar las políticas públicas desde una perspectiva de derechos humanos, incorporando evaluaciones de impacto de salud mental y el principio de autonomía progresiva en el tratamiento de datos de la infancia.

El análisis de los resultados en el segundo capítulo puso de relieve cómo la confluencia de factores psicosociales y tecnológicos incrementa la vulnerabilidad de niños, niñas y adolescentes. La ausencia de educación digital crítica y de supervisión parental potencia la sexualización temprana, la ansiedad y la depresión, al exponer a los menores a pornografía y estándares inalcanzables de belleza, lo que favorece la baja autoestima y los trastornos alimentarios. A su vez, el hiperconsumo y la violencia digital se retroalimentan de la explotación de inseguridades adolescentes, en un entorno sin sanciones efectivas ni límites de uso adecuados. La hiperconectividad acelerada por la pandemia, lejos de aliviar el aislamiento, ha generado dependencia de las notificaciones, fatiga emocional y estrés familiar, lo que subraya la necesidad de reforzar el acompañamiento psicosocial y las redes de apoyo comunitario.

Por otro lado, la corresponsabilidad entre familia, Estado y empresas digitales se muestra fragmentada. Mientras las familias carecen de alfabetización digital, el Estado no asegura atención psicológica universal ni educación mediática, y las empresas priorizan intereses económicos. Esta descoordinación impide que iniciativas como “Internet Segura” se traduzcan en entornos preventivos. En materia de protección de datos, aunque existen marcos de protección normativa como la LOPDP y el RGPD de referencia, la escasez de recursos de la Superintendencia de Protección de Datos y la falta de evaluaciones de impacto por parte de muchas plataformas evidencian una brecha significativa entre norma y práctica. Las respuestas alternativas proponen alianzas

internacionales, políticas nacionales de educación digital y salud mental, y una cultura organizacional responsable, con el fin de construir espacios digitales seguros y cerrar de manera integral las brechas de riesgo que enfrentan los NNA.

El tercer capítulo identifica que la exigibilidad del derecho a la salud mental de niños, niñas y adolescentes en el entorno digital requiere una aproximación multifacética, que articule acciones jurídicas, sociales, políticas e internacionales. Se reconoce que el marco constitucional ecuatoriano ya otorga jerarquía a la protección de datos personales, lo cual habilita recursos como el hábeas data, el litigio estratégico y los reclamos administrativos ante la Superintendencia de Protección de Datos. Sin embargo, estos mecanismos aún no se han activado plenamente en casos que involucren a NNA, lo que refleja una subutilización del potencial jurídico disponible. El capítulo también resalta la importancia de documentar casos emblemáticos (como el uso de datos biométricos en la plataforma *Worldcoin*) para establecer precedentes, evidenciar violaciones estructurales y motivar acciones judiciales de alto impacto.

Asimismo, se plantea que el litigio estratégico solo puede ser efectivo si se combina con acciones sostenidas desde la sociedad civil, campañas de sensibilización, educación digital y presión mediática. La exigibilidad política se presenta como una herramienta clave, en la medida en que permite interpelar a autoridades, promover reformas normativas y posicionar el tema en la agenda pública, especialmente en procesos electorales o de fiscalización parlamentaria. A nivel internacional, se propone activar mecanismos del sistema de Naciones Unidas y del Sistema Interamericano de Derechos Humanos, así como fortalecer alianzas con organizaciones como *Privacy International* o la APC. En conjunto, el capítulo no solo mapea rutas de acción, sino que sienta las bases para seguir explorando y fortaleciendo mecanismos de exigibilidad, con el objetivo de garantizar una protección efectiva de los derechos digitales y la salud mental de la infancia y adolescencia en un entorno tecnológico cada vez más invasivo y desregulado.

Sin embargo, varios nudos críticos limitan la efectividad de estas estrategias en el contexto ecuatoriano. La desconexión entre la LOPDP y la LOSM impide protocolos específicos para NNA; la escasa alfabetización digital de familias y docentes dificulta la identificación y denuncia de prácticas invasivas; la Superintendencia carece de recursos técnicos y autonomía política para supervisar plataformas transnacionales; y el poder económico de las grandes tecnológicas excede con mucho la capacidad regulatoria de un solo Estado, lo que obliga a buscar alianzas y normas internacionales vinculantes.

El trabajo también reconoce sus propias limitaciones. Conceptualmente, se centró en un enfoque crítico de derechos humanos, sin profundizar en modelos clínicos de diagnóstico psicológico ni en intervenciones terapéuticas específicas. Metodológicamente, la muestra de nueve informantes (aunque diversa en experticia) no incluye voces directas de niños, niñas o adolescentes, cuyas aportaciones éticas y metodológicas requieren protocolos especiales. Además, el corte temporal de los datos (hasta junio de 2024) no capta evoluciones recientes ni escenarios de zonas rurales muy aisladas, donde la conectividad y los riesgos digitales pueden presentar matices distintos.

De cara a futuras investigaciones, es esencial combinar estudios cuantitativos y cualitativos. Por ejemplo, en áreas como la medición de ansiedad, depresión o adicción digital se requieren escalas clínicas validadas, mientras que las investigaciones participativas con niños, niñas y adolescentes pueden profundizar las estrategias de autorregulación y perspectivas sobre el entorno digital. Un análisis comparado con otros países latinoamericanos aportaría aprendizajes sobre modelos articulados de datos y salud mental, y la evaluación sistemática de intervenciones educativas y litigios estratégicos permitiría medir su efectividad en términos de concientización y cambios normativos.

En suma, la protección de los datos personales y la salud mental de niños, niñas y adolescentes en la era digital exige un enfoque integral. Sólo mediante la coordinación efectiva de marcos legales, la capacitación de la sociedad civil, la presión normativa y el monitoreo continuo de las plataformas se podrá garantizar que la tecnología sirva para potenciar, y no para vulnerar, los derechos de la población más joven. Asimismo, este estudio ofrece un punto de partida (teórico, normativo y práctico) que puede orientar a la sociedad civil, la academia y las entidades estatales en la exploración y el perfeccionamiento de mecanismos de exigibilidad, con el fin de que la protección de datos personales contribuya de manera más efectiva al bienestar psicológico de la infancia y la adolescencia en Ecuador.

# Bibliografía

ACNUDH. “Comité de Derechos Humanos”. *OHCHR*. Accedido 16 de septiembre de 2020. https://www.ohchr.org/SP/HRBodies/CCPR/Pages/CCPRIndex.aspx.

———. “Relator Especial sobre el derecho a la privacidad”. *OHCHR*. Accedido 17 de septiembre de 2020. https://www.ohchr.org/SP/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx.

Agencia Española de Protección de Datos. "La Agencia Española de Protección de Datos se suma a la Carta de Derechos Digitales de Niños, Niñas y Adolescentes promovida por la Fundación Anar", 9 de septiembre de 2019. https://www.aepd.es/prensa-y-comunicacion/notas-de-prensa/la-agencia-espanola-de-proteccion-de-datos-se-suma-la-carta.

Alcántara, José. “El panóptico, la cárcel perfecta de Jeremy Bentham”. *Versvs*, 11 de abril de 2007. https://www.versvs.net/panoptico-carcel-perfecta-jeremy-bentham/.

Anaya Muñoz, Alejandro. “La construcción internacional de los Derechos Humanos: El papel de las Relaciones Internacionales”. *Revista de Relaciones Internacionales de la UNAM* 0, n.º 104 (2010). http://www.revistas.unam.mx/index.php/rri/article/view/18132, 10.

Article 29 Data Protection Working Party. “Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is ‘likely to result in a high risk’ for the purposes of Regulation 2016/679”, 4 de abril de 2017. https://ec.europa.eu/newsroom/document.cfm?doc_id=44137.

———. “About Privacy International”. *Privacy International*. Accedido 9 de noviembre de 2021. https://www.privacyinternational.org/about.

BBC. “Learning - What Is An Algorithm”. *BBC*. 2015. https://www.youtube.com/watch?v=Da5TOXCwLSg.

BBC News Mundo. "Zuckerberg: el jefe de Facebook se disculpa ante las familias de los niños que han sufrido daños por culpa de las redes sociales". *BBC News Mundo*, 1 de febrero de 2024. https://www.bbc.com/mundo/articles/c72gze8r05jo.

Bonilla-Morejón, Diego Marcelo, y Delia Paulina Samaniego-Quiguiri. «Evolución y desafíos de la protección de datos personales en el contexto de la globalización».

*Horizon Nexus Journal* 2, n.º 1 (31 de enero de 2024): 62-74. doi:10.70881/hnj/v2/n1/34.

Blasco, Lucía. "Qué es el 'oscuro' capitalismo de la vigilancia de Facebook y Google y por qué lo comparan con la conquista española". *BBC News Mundo*. 1 de marzo de 2019. https://www.bbc.com/mundo/noticias-47372336.

Clarín. "Byung-Chul Han: vamos hacia un feudalismo digital y el modelo chino podría imponerse". *Periódico*. 14 de abril de 2020. https://www.clarin.com/cultura/byung-chul-vamos-feudalismo-digital-modelo-chino-podria-imponerse_0_QqOkCraxD.html?fbclid=IwAR0dXGUP0PLeyHLfDZed_aLWp9eaD5BpUpHbpVcY5RqAg1eFJgW0fx5TtNI.

Cana, Daniel. "¿Por qué los datos de las personas normales valen más que el petroleo?" *Thingeer*. 9 de agosto de 2019. https://blog.thingeer.com/por-que-los-datos-de-las-personas-normales-valen-mas-que-el-petroleo/.

Cárdenas Gutiérrez, Diana Janely. "Consecuencias Psicológicas del uso Excesivo de las Redes Sociales en Niños y Jóvenes". Universidad Católica de Cuenca, 2024. https://dspace.ucacue.edu.ec/bitstreams/083878dc-cf9c-41bd-b7ca-68cf9ccfd21f/download.

Centre for Mental Health. "Impacto de las redes sociales sobre la salud mental de los jóvenes, según el Centre for Mental Health". *InfoCop Online-Revista de Psicología* (2018). http://www.infocop.es/print.asp?print=yes.

Centro de Biotecnología. "¿Qué es la biotecnología?". *Centro de Biotecnología*. 12 de noviembre de 2019. https://www.centrobiotecnologia.cl/comunidad/que-es-la-biotecnologia/.

CEPAL, y UNESCO. "La educación en tiempos de la pandemia de COVID-19", agosto de 2020. https://repositorio.cepal.org/server/api/core/bitstreams/c29b3843-bd8f-4796-8c6d-5fcb9c139449/content.

Cepeda, José Alejandro. "Foucault y la naturaleza circular del poder". *Diálogo Político*, 11 de agosto de 2015. https://dialogopolitico.org/actualidad/foucault-y-la-naturaleza-circular-del-poder/.

Cevallos, y Gabriela Paulina León Burgos. "La protección de datos personales en Ecuador". *Estudios del Desarrollo Social: Cuba y América Latina* 10, n.º especial 1 (2022). https://revistas.uh.cu/revflacso/article/view/3594.

CIDH, Relatoría Especial para la Libertad de Expresión. “Estándares para una Internet Libre, Abierta e Incluyente”. *CIDH*. 15 de marzo de 2017. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiQyKKHgc_rAhWGwVkKHfr2BxAQFjAAegQIBxAB&url=http%3A%2F%2Fwww.oas.org%2Fes%2Fcidh%2Fexpresion%2Fdocs%2Fpublicaciones%2Finternet_2016_esp.pdf&usg=AOvVaw3NnuAYlvGay9-fr_a8dyMC.

CNN Chile. “Corte admite recurso contra empresa internacional por escaneo del iris a menor de edad a cambio de criptomonedas”. *CNN Chile*. Accedido 15 de agosto de 2024. https://www.cnnchile.com/pais/corte-recurso-proteccion-menor-de-edad-datos-biometricos-iris-criptomonedas_20240325/.

Colombia Corte Constitucional. “Sentencia T-881-02”. 17 de octubre de 2002. http://www.corteconstitucional.gov.co/relatoria/2002/t-881-02.htm.

Comisión Interamericana de Derechos Humanos. “CIDH: Información sobre audiencias”. *Comisión Interamericana de Derechos Humanos (CIDH)*. Accedido 27 de septiembre de 2024. https://www.oas.org/es/CIDH/jsForm/?File=/es/cidh/sesiones/coberturas.asp.

———. “CIDH: Sesiones”. *Comisión Interamericana de Derechos Humanos (CIDH)*. *OAS*. Accedido 27 de septiembre de 2024. https://www.oas.org/es/cidh/sesiones/default.asp.

———. “Informe Empresas y Derechos Humanos: Estándares Interamericanos”. *Canal CIDH*, 1 de noviembre de 2019. CIDH/REDESCA/INF.1/19.

———. “Períodos de Sesiones”. *Canal CIDH*. Accedido 27 de septiembre de 2024. https://www.canalcidh.org/periodos-de-sesiones.

———. “¿Qué es la CIDH?” *Comisión Interamericana de Derechos Humanos (CIDH)*. Accedido 20 de septiembre de 2024. https://www.oas.org/es/CIDH/jsForm/?File=/es/cidh/mandato/que.asp.

Comité de Derechos Económicos, Sociales y Culturales. “Observación General No. 14: El derecho al disfrute del más alto nivel posible de salud”. 11 de agosto de 200d. C. 22° período de sesiones.

Comité de Derechos Humanos. “Observación General Nro. 16: Derecho a la intimidad (Art. 17)”, 1988.

Comité de los Derechos del Niño. “Lista de Cuestiones previa a la presentación del séptimo informe periódico del Ecuador”. 28 de octubre de 2021. CRC/C/ECU/QPR/7.

———. “Observación General N°15 (2013) sobre el derecho del niño al disfrute del más alto nivel posible de salud (artículo 24)”. 17 de abril de 2013. CRC/C/GC/15.

———. "Observación general núm. 25 (2021) relativa a los derechos de los niños en relación con el entorno digital", 2 de marzo de 2021. CRC/C/GC/25.

———. "Observaciones finales sobre el séptimo informe periódico del Ecuador", 27 de febrero de 2025. CRC/C/ECU/CO/7.

———. “Observaciones finales sobre los informes periódicos quinto y sexto combinados del Ecuador”, 26 de octubre de 2017. CRC/C/ECU/CO/5-6.

———. "Séptimo informe periódico que el Ecuador debía presentar en 2023 en virtud del artículo 44 de la Convención", 13 de febrero de 2024. CRC/C/ECU/7.

Consejo de Derechos Humanos. "El papel de los determinantes de la salud en el avance del derecho a la salud mental. Informe del Relator Especial sobre el derecho de toda persona al disfrute del más alto nivel posible de salud física y mental", 12 de abril de 2019. A/HRC/41/34.

———. "Informe al Consejo de Derechos Humanos (enfoque principal: derecho a la salud de los adolescentes). Informe del Relator Especial sobre el derecho de toda persona al disfrute del más alto nivel posible de salud física y mental", 4 de abril de 2016. A/HRC/32/32.

———. "Informe del RE sobre el derecho a la salud mental", 28 de marzo de 2017. A/HRC/35/21.

———. "Innovación digital, tecnologías y derecho a la salud. Informe de la Relatora Especial sobre el derecho de toda persona al disfrute del más alto nivel posible de salud física y mental", 21 de abril de 2023. A/HRC/53/65.

———. "Salud mental y derechos humanos: Establecer una agenda global basada en los derechos. Informe de la Relatora Especial sobre el derecho de toda persona al disfrute del más alto nivel posible de salud física y mental", 15 de abril de 2020. A/HRC/44/48.

Consejo de Participación Ciudadana y Control Social. “Fabrizio Peralta Díaz es el primer superintendente de Protección de Datos”. *CPCCS*. Accedido 1 de mayo de 2024. https://www.cpccs.gob.ec/2024/03/fabrizio-peralta-superintendente/.

———. “Proceso de Selección del Superintendente de Protección de Datos”. *CPCCS*. Accedido 1 de marzo de 2024. https://www.cpccs.gob.ec/designacion-de-autoridades/super-proteccion-datos/.

Consejo Europeo. “Convention for the protection of individuals with regard to the processing of personal data”. Junio de 2018.

———. “Details of Treaty No.108”. *Treaty Office*. Accedido 7 de octubre de 2024. https://www.coe.int/en/web/conventions/full-list.

———. “Modernisation of Convention 108”. *Data Protection*. Accedido 10 de octubre de 2024. https://www.coe.int/es/web/data-protection/convention108/modernised.

Consejo Nacional para la Igualdad Intergeneracional. “Política Pública pro una Internet Segura para niños, niñas y adolescentes”. Septiembre de 2020.

“Convenio sobre Diversidad Biológica”, 2 de noviembre de 2006. https://www.cbd.int/convention/articles/?a=cbd-02.

Coordinación de Universidad Abierta y Educación a Distancia, Unam. “Problemas y Algoritmos”. *Cuaed*. s.f. https://programas.cuaed.unam.mx/repositorio/moodle/pluginfile.php/1163/mod_resource/content/1/contenido/index.html.

Coronel Altamirano, Renato. “Worldcoin: Autenticación de Humanos vs. Protección de Datos Personales”. 14 de marzo de 2024. https://n9.cl/ecugd.

Corte Constitucional del Ecuador. Caso No. 2064-14-EP/21, Sentencia No. 2064-14-EP/21 § (2021).

Corte Interamericana de Derechos Humanos. “ABC de la Corte Interamericana de Derechos Humanos”. 2018. https://repositorio.consejodecomunicacion.gob.ec/bitstream/CONSEJO_REP/1138/1/ABCCorteIDH.pdf.

———. Caso Miembros de la Corporación Colectivo de Abogados “José Alvear Restrepo” Vs. Colombia (18 de octubre de 2023).

———. “Reglamento de la Corte Interamericana de Derechos Humanos”. Noviembre de 2009. https://www.corteidh.or.cr/sitios/reglamento/nov_2009_esp.pdf.

De la Torre, Rosa Elena, y Juan Montaña Pinto. “El habeas data en Ecuador”. En *Apuntes de derecho procesal constitucional*, 179-92. T. 2. Quito-Ecuador: CEDEC, 2012.

Demetzou, Katerina. “GDPR and the Concept of Risk: The Role of Risk, the Scope of Risk and the Technology Involved”. En *Privacy and Identity Management. Fairness, Accountability, and Transparency in the Age of Big Data*, editado por Eleni Kosta, Jo Pierson, Daniel Slamanig, Simone Fischer-Hübner, y Stephan Krenn, 547:137-54. IFIP Advances in Information and Communication

Technology. Cham: Springer International Publishing, 2019. doi:10.1007/978-3-030-16744-8_10.

Derechos Digitales. “Derechos Digitales”. *Derechos Digitales*. Accedido 9 de noviembre de 2021. https://www.derechosdigitales.org/quienes-somos/derechos-digitales/.

Derechos Digitales América Latina. “Contribuciones sobre derechos humanos en el entorno digital en Ecuador”, 2022.

Derechos Digitales América Latina, De Souza Michel. “Ecuador: muchos cambios, poco que celebrar”. *Derechos Digitales*. 12 de mayo de 2023. https://www.derechosdigitales.org/20752/ecuador-muchos-cambios-poco-que-celebrar/.

DataReportal – Global Digital Insights. “Digital 2024: Ecuador”. *DataReportal*. 23 de febrero de 2024. https://datareportal.com/reports/digital-2024-ecuador.

Discovery en Español. “¿Sabes qué es BIG DATA?”. *Vídeo de YouTube*. 2020. https://www.youtube.com/watch?v=Ju2oDsHAL-o.

DW Documental “Google, Facebook, Amazon - El poder ilimitado de los consorcios digitales”. *Vídeo de YouTube*. 2022. https://www.youtube.com/watch?v=A3cGMNxRNJ0.

DW Documental. “La comercialización de la propia imagen: los peligros de las redes sociales”. *Vídeo de YouTube*. 2022. https://www.youtube.com/watch?v=DWqLAlsiPbE.

DW Documental. “Multitasking - ¿Cuánto se puede hacer al mismo tiempo”. *Vídeo de YouTube*. 2022. https://www.youtube.com/watch?v=qGQwvd6bd1I.

DW Español. “Cómo las redes sociales enturbian nuestra visión del futuro El uso excesivo de las redes sociales puede afectar a nuestra salud mental y llevarnos a una visión sombría de la vida. Así es como puedes evitarlo. #DWDigital #DWMagacines https://t.co/uZXBi3pZdS”. Tweet. *Twitter*, 13 de mayo de 2024. https://x.com/dw_espanol/status/1790124198989385879.

Ecuador. *Código Civil*. Registro Oficial 46, Suplemento, 24 de junio de 2005.

———. *Constitución de la República del Ecuador*. Registro Oficial 449, 20 de octubre de 2008.

———. *Decreto Ejecutivo 904*. Registro Oficial 435, Suplemento, 13 de noviembre de 2023.

———. Fiscalía General del Estado. "Políticas y Directrices Institucionales". Accedido 27 de abril de 2025. https://www.fiscalia.gob.ec/politicas-y-directrices-institucionales/.

———. INEC. "Desigualdades Educativas en el contexto de la pandemia de la COVID-19 en el Ecuador", junio de 2022. https://www.ecuadorencifras.gob.ec/documentos/web-inec/Bibliotecas/Libros/Reportes/Educacion_COVID.pdf.

———. *Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional*. Registro Oficial 52, Suplemento, 22 de octubre de 2009.

———. *Ley Orgánica de Salud Mental*. Registro Oficial 471, Suplemento, 5 de enero de 2024.

———. *Ley Orgánica de la Función Legislativa*. Registro Oficial 642, Suplemento, 29 de julio de 2009.

———. *Ley Orgánica para la Trasformación Digital y Audiovisual*. Registro Oficial 245, Tercer Suplemento, 7 de febrero de 2023.

———. *Ley Orgánica Reformatoria a varios Cuerpos Legales para el Fortalecimiento de las Capacidades Institucionales y la Seguridad Integral*. Registro Oficial 279, Suplemento, 29 de marzo de 2023.

———. *Ley Orgánica de Protección de Datos Personales*. Registro Oficial 459, Suplemento, 26 de mayo de 2021.

———. Ministerio de Educación. "Política Nacional de Convivencia Escolar", 12 de marzo de 2021. https://educacion.gob.ec/wp-content/uploads/downloads/2021/04/Politica-Nacional-de-Convivencia-Escolar.pdf.

Ecuador, Presidencia. "Más de 82.000 personas recibieron atención en salud mental durante la Emergencia Sanitaria – Presidencia de la República del Ecuador", s.f. https://www.presidencia.gob.ec/mas-de-82-000-personas-recibieron-atencion-en-salud-mental-durante-la-emergencia-sanitaria/.

———. *Reglamento General a la Ley Orgánica de Salud Mental*. Decreto Ejecutivo No. 465 § (2024). Registro Oficial Suplemento 697, 4 de diciembre de 2024.

Ecuavisa. “Ecuatorianos escanean su iris a cambio de criptomonedas”. *Vídeo de YouTube*. 2024. https://www.youtube.com/watch?v=eS4K2SI0TDE.

EDPB. “Legado: Grupo de Trabajo del art. 29”. *European Data Protection Board*. Accedido 14 de agosto de 2024. https://www.edpb.europa.eu/about-edpb/who-we-are/legacy-art-29-working-party_es.

Egas, Verónica, Lenín Jácome Chávez, y Luis Iriarte. “¿Por qué no funciona la Ley de Salud Mental?” Presentado en Conversatorio de Salud Mental, Quito-Ecuador, 10 de abril de 2025. https://www.instagram.com/reel/DIjRukGuX9o/?igsh=MXQ0cDltNmRodHhzOQ%3D%3D.

elEconomista.es. “Worldcoin, la polémica empresa que escaneaba el iris de menores por criptomonedas cesa su actividad en España”. *elEconomista.es*. 4 de junio de 2024. https://www.eleconomista.es/actualidad/noticias/12848184/06/24/worldcoin-la-polemica-empresa-que-escaneaba-el-iris-de-menores-por-criptomonedas-cesa-su-actividad-en-espana.html.

El Comercio. “La Policía arresta a gerente de Novaestrat, por supuesta filtración de datos de ecuatorianos”. *El Comercio*. Accedido 25 de septiembre de 2020. http://www.elcomercio.com/actualidad/policia-arresto-gerente-novaestrat-filtracion.html.

El Universo. “Cientos permiten escaneo de sus iris por ‘bono’ en criptomonedas de Worldcoin, en Guayaquil y Quito”. *El Universo*. 2024. https://www.youtube.com/watch?v=j7Pld5mJ3LU.

Enríquez Álvarez, Luis. “La Visión de América Latina sobre el Reglamento General de Protección de Datos”. *Comentario Internacional* n.° 19 (2019): 99-112. doi:10.32719/26312549.2019.19.4.

Escurra Mayaute, Miguel, y Edwin Salas Blas. “Construcción y validación del cuestionario de adicción a redes sociales”. *Universidad Nacional Mayor de San Marcos, Perú. Universidad de San Martín de Porres, Perú*, 2014, 73-91.

Ferrajoli, Luigi, Perfecto Andrés Ibáñez, y Andrea Greppi. *Derechos y garantías: La ley del más débil*, 7.ª ed. Madrid: Trotta, 2010.

Fernández-Rovira, Cristina. “Motivaciones y tiempo de uso de las redes sociales por parte de los jóvenes españoles: señales de adicción”. *Anuario Electrónico de Estudios en Comunicación Social “Disertaciones”* 15, n.º 2 (11 de julio de 2022). doi:10.12804/revistas.urosario.edu.co/disertaciones/a.11155.

Ferrajoli, Luigi, Perfecto Andrés Ibáñez, y Andrea Greppi. *Derechos y garantías: La ley del más débil*, 7. ed. Madrid: Trotta, 2010.

Flacso. “Violaciones, derechos humanos y contexto: herramientas propuestas para documentar e investigar. Manual de Análisis de Contexto para Casos de Violaciones a los Derechos Humanos”. International Bar Association’s Human Rights Institute, 2017.

Fundamedios. “30 dólares por escanear tu iris: ¿vale la pena?”. *Vídeo de YouTube*. Accedido 15 de agosto de 2024. https://www.youtube.com/watch?v=UoHqcGYL3Eg.

Fung, Clare Duffy, Brian. «Mark Zuckerberg se disculpa con familias por los daños causados en redes sociales». *CNN*, 31 de enero de 2024. https://cnnespanol.cnn.com/2024/01/31/mark-zuckerberg-se-disculpa-familias-danos-causados-redes-sociales-trax.

FXSSI - Indicador de Sentimiento de Forex. “Las empresas más valiosas del mundo - 2019”. Accedido 19 de noviembre de 2019. https://es.fxssi.com/las-empresas-mas-valiosas-del-mundo.

Gellert, Raphaël. *The Risk-Based Approach to Data Protection*. Oxford: Oxford Scholarship Online, 2020. https://doi.org/10.1093/oso/9780198837718.001.0001.

Giraldo-Luque, Santiago, y Cristina Fernández-Rovira. “Redes sociales y consumo digital en jóvenes universitarios: economía de la atención y oligopolios de la comunicación en el siglo XXI”. *Profesional de la información* 29, n.º 5 (3 de noviembre de 2020). doi:10.3145/epi.2020.sep.28.

GKA Comunicación. “Exigibilidad de los derechos”. *Vídeo de YouTube*. 2014. https://www.youtube.com/watch?v=N0oPTSns8tQ.

Gobierno de Argentina. “Se convirtió en Ley la aprobación del Convenio 108+”. *REDIPD*. 30 de noviembre de 2022. https://www.redipd.org/es/noticias/se-convirtio-en-ley-la-aprobacion-del-convenio-108.

Godoy, Lorena Naranjo. “Internet segura para la niñez y adolescencia”. *El Comercio*. 13 de mayo de 2024. https://www.elcomercio.com/opinion/internet-segura-para-ninez-adolescencia-lorena-godoy-columnista.html.

Grupo “Protección De Datos” Del Artículo 29. “Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento ‘entraña probablemente un alto riesgo’ a efectos del Reglamento (UE) 2016/679”. *AEPD*. 4 de octubre de 2019. https://www.aepd.es/sites/default/files/2019-09/wp248rev01-es.pdf.

Han, Byung-Chul. “Psicopolítica: Neoliberalismo y nuevas técnicas de poder”. *Ebsco*. 2014. https://search.ebscohost.com/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=1544689.

Harari, Yuval Noah. *21 lecciones para el siglo XXI*. Colombia: Penguin Random House, 2018.

———. “El Antropoceno”. En *Homo Deus: Breve historia del mañana*, 87-117. Colombia: Penguin Random House, 2018.

———. “Religión”. “En 21 lecciones para el siglo XXI”, 149-79. Colombia: Penguin Random House, s. f.

Heffler, Karen Frankel, Binod Acharya, Keshab Subedi, y David S. Bennett. “Early-Life Digital Media Experiences and Development of Atypical Sensory Processing”. *JAMA Pediatrics* 178, n.º 3 (1 de marzo de 2024): 266. doi:10.1001/jamapediatrics.2023.5923.

Instituto Interamericano de Derechos Humanos. Inclusión, derechos humanos e incidencia política. Serie Módulos educativos 5. San José, Costa Rica: IIDH, Inst. Interamericano de Derechos Humanos, 2004.

Instituto Nacional de Estadística y Censos. “Tecnologías de la Información y Comunicación 2020”. *INEC*. abril de 2021. https://www.ecuadorencifras.gob.ec/documentos/web-inec/Estadisticas_Sociales/TIC/2020/202012_Principales_resultados_Multiproposito_TIC.pdf.

———. “Tecnologías de la Información y Comunicación-TIC”. *INEC*. 2 de mayo de 2021. https://n9.cl/dh04.

Instituto Nacional de Estadística y Censos. “Censo Ecuador 2022”. *INEC. Censo Ecuador*, 2023. https://www.censoecuador.gob.ec/.

Johnson, Douglas. “La Necesidad de Nuevas Tácticas”. *Nonviolent*. Marzo de 2004. https://www.nonviolent-conflict.org/wp-content/uploads/2017/01/The-Need-for-New-tactics-Spanish.pdf.

Khan Academy. “Algoritmos | Ciencias de la computación”. *Khan Academy*. Accedido 6 de junio de 2023. https://es.khanacademy.org/computing/computer-science/algorithms.

Konok, V., M.-A. Binet, Á. Korom, Á. Pogány, Á. Miklósi, y C. Fitzpatrick. “Cure for Tantrums? Longitudinal Associations between Parental Digital Emotion

Regulation and Children's Self-Regulatory Skills". *Frontiers in Child and Adolescent Psychiatry* 3 (28 de junio de 2024): 1276154. doi:10.3389/frcha.2024.1276154.

La Vanguardia. "EE.UU. denuncia a Facebook e Instagram por dañar la salud mental de los niños a sabiendas". *La Vanguardia*. 26 de octubre de 2023. https://www.lavanguardia.com/vida/20231026/9329037/eeuu-denuncia-facebook-instagram-danar-salud-mental-ninos-sabiendas.html.

Lagos, Anna. "Worldcoin llega a México y establece una economía paralela a cambio de datos personales". *WIRED*. 29 de mayo de 2024. https://es.wired.com/articulos/worldcoin-llega-a-mexico-y-establece-una-economia-paralela-a-cambio-de-datos-personales.

Majaz". Primera edición. Lima: Fedepaz/Oxfam, 2015.

Malan, David J. "Tu cerebro puede hacer algoritmos", 2013. https://www.youtube.com/watch?v=6hfOvs8pY1k.

Malgieri, Gianclaudio. *Vulnerability and Data Protection Law*. United Kingdom: Oxford University Press, 2023. https://global.oup.com/academic/product/vulnerability-and-data-protection-law-9780192870339?cc=ec&lang=en&.

Martínez, Mario Ramiro Aguilar, Julio Alfredo Paredes López, Diego Patricio Gordillo

Meaker, Morgan. "A Danish City Built Google Into Its Schools—Then Banned It". *Wired*. Accedido 5 de mayo de 2025. https://www.wired.com/story/denmark-google-schools-data/.

Medrano, Juan Carlos Andrade, y Patricio Iván Rosas Flores. "Las Redes Sociales como Lugar de Construcción de Contrapoder", 2017.

Melo Cevallos, Mario, y Justicia y Sociedad (Bogotá Centro de Estudios de Derecho Colombia). Sarayaku ante el sistema interamericano de derechos humanos: justicia para el pueblo del Medio Día y su selva viviente, 2016.

Melish, Tara. "Capítulo 5. Estableciendo la responsabilidad del Estado: El deber de respetar, el deber de garantizar y el principio de progresividad (Arts. 1, 2 y 26)". En *La Protección de los derechos económicos, sociales y culturales en el sistema interamericano*, 171-211. Quito: CDES, 2003.

Ministerio de la Mujer y Derechos Humanos. "Subsecretaría de Derechos Humanos". *Ministerio de la Mujer y Derechos Humanos*. 6 de noviembre de 2019. https://www.derechoshumanos.gob.ec/subsecretaria-de-derechos-humanos-ec/.

Ministerio de Telecomunicaciones y de la Sociedad de la Información. Política de Ciberseguridad, Acuerdo Ministerial 006-2021 § (2021). https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Acuerdo-No.-006-2021-Politica-de-Ciberseguridad.pdf.

Moreira de Freitas, Rodrigo Jácob, Thaisa Natália Carvalho Oliveira, Juce Ally Lopes de Melo, Jennifer do Vale e Silva, Kísia Cristina de Oliveira e Melo, Samara Fontes Fernandes, Rodrigo Jácob Moreira de Freitas, et al. "Percepciones de los adolescentes sobre el uso de las redes sociales y su influencia en la salud mental". *Enfermería Global* 20, n.º 64 (2021): 324-64. doi:10.6018/eglobal.462631.

Naranjo Godoy, Lorena. "El dato personal como presupuesto del derecho a la protección de datos personales y del hábeas data en Ecuador". *Foro. Revista de Derecho* 27 (2017): 63-82.

———. "Los riesgos de entregar datos biométricos personales como el iris". *El Comercio*, 2 de agosto de 2024. https://www.elcomercio.com/?p=1423127.

———. "Ponencia: Proyecto de ley de protección de datos personales". Presentado en Curso sobre Derecho Digital de la Facultad de Jurisprudencia de la PUCE. Accedido 23 de septiembre de 2020. https://www.facebook.com/salim.zaidan/videos/10157069142610896/.

Nativa Digital. "La Amenaza Silenciosa del Escaneo de Iris en Menores". Accedido 15 de agosto de 2024. https://nativadigital.org/la-amenaza-silenciosa-del-escaneo-de-iris-en-menores/.

Netflix. "Nada Es Privado. Documental", 2019. https://www.netflix.com/watch/80117542?trackId=13752289&tctx=0%2C0%2C6eba89d7-924d-46fb-b19a-ea1cc2e03a55-16740837%2C%2C.

Netflix. "The Social Dilemma", 2020. https://n9.cl/rl1mz.

OEA. "CIDH: Relatoría Especial sobre los Derechos Económicos, Sociales, Culturales y Ambientales". *Comisión Interamericana de Derechos Humanos (CIDH)*. Accedido 27 de septiembre de 2024. https://www.oas.org/es/CIDH/jsForm/?File=/es/cidh/r/DESCA/default.asp.

———. "CIDH: Relatoría sobre los Derechos de la Niñez". *Comisión Interamericana de Derechos Humanos (CIDH)*. Accedido 27 de septiembre de 2024. https://www.oas.org/es/CIDH/jsForm/?File=/es/cidh/r/DN/default.asp.

———. “CIDH: Relatoría sobre los Derechos de las Mujeres”. *Comisión Interamericana de Derechos Humanos (CIDH)*. Accedido 27 de septiembre de 2024. https://www.oas.org/es/CIDH/jsForm/?File=/es/cidh/r/DMUJERES/default.asp.

———. “Relatorías y Unidades Temáticas”. Text. Accedido 27 de septiembre de 2024. https://www.oas.org/es/CIDH/mandato/relatorias.asp.

———.Comité Jurídico Interamericano. Principios Actualizados del Comité Jurídico Interamericano sobre la Privacidad y la Protección de Datos Personales, con Anotaciones, Pub. L. No. CJI/DOC.638/21 (2021).

Oficina del Alto Comisionado de Naciones Unidas. “Acerca del CDH”. *OHCHR*. Accedido 20 de septiembre de 2024. https://www.ohchr.org/es/hr-bodies/hrc/about-council.

———. *El sistema de tratados de derechos humanos de las Naciones Unidas*. Folleto informativo Nro. 30/Rev. 1. Nueva York y Ginebra, 2012. https://www.ohchr.org/Documents/Publications/FactSheet30Rev1_sp.pdf.

———. “Mecanismos y entidades del Consejo de Derechos Humanos”. *OHCHR*. Accedido 20 de septiembre de 2024. https://www.ohchr.org/es/hr-bodies/hrc/other-sub-bodies.

Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. “Notificación de violaciones”. *OHCHR*. Accedido 16 de septiembre de 2024. https://www.ohchr.org/es/reporting_violations.

———. “Special Procedures Thematic mandates”. Accedido 17 de septiembre de 2024. https://spinternet.ohchr.org/ViewAllCountryMandates.aspx?Type=TM&lang=sp

Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos en México. El litigio estratégico en México: la aplicación de los derechos humanos a nivel práctico: experencias de la sociedad civil. México, D.F.: Oficinia en México del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, 2007.

———.*la aplicación de los derechos humanos a nivel práctico : experencias de la sociedad civil.* México, D.F.: Oficinia en México del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, 2007.

OHCHR. “4th UPR Cycle: Contributions and Participation of “Other Stakeholders” in the UPR”. Accedido 20 de septiembre de 2024. https://www.ohchr.org/en/hr-bodies/upr/ngos-nhris.

ONU Asamblea General. “Aprovechar las oportunidades de sistemas seguros, protegidos y fiables de inteligencia artificial para el desarrollo sostenible”, 11 de marzo de 2024. A/78/L.49.

———. “Convención sobre Eliminación de toda Discriminación contra la Mujer”, 18 de octubre de 1979.

———. “Convención sobre los Derechos del Niño”, 20 de diciembre de 1989. Resolución 44/25.

———. “Declaración Universal de Derechos Humanos”, 10 de diciembre de 1948. Resolución 217 (A) III.

———. “Pacto Internacional de Derechos Civiles y Políticos”, 16 de diciembre de 1966. Resolución 2200A (XXI).

———. “Pacto Internacional de Derechos Económicos, Sociales y Culturales”, 16 de diciembre de 1966.

———. “Promoción y protección del derecho a la libertad de opinión y expresión. Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión”, 29 de agosto de 2018. A/73/348*.

ONU Consejo de Derechos Humanos. “El derecho a la privacidad en la era digital”, 3 de agosto de 2018. A/HRC/39/29.

———. “Informe del Relator Especial sobre el Derecho a la Privacidad”, 16 de octubre de 2019. A/HRC/40/63.

———. “Principios Rectores sobre las Empresas y los Derechos Humanos”, 15 de junio de 2011. HR/PUB/11/04.

ONU Mujeres. “Hechos y cifras: Poner fin a la violencia contra las mujeres”. Accedido 23 de julio de 2024. https://www.unwomen.org/es/what-we-do/ending-violence-against-women/facts-and-figures.

Organizaciones de la Sociedad Civil de Latinoamérica. “Declaración de Quito acerca de la exigibilidad y realización de los derechos económicos, sociales y culturales (DESC) en América Latina y el Caribe”, 24 de julio de 1998. http://www.derechos.org.ve/pw/wp-content/uploads/desc_01.pdf.

Organización de los Estados Americanos. “Convención Americana sobre Derechos Humanos”, 22 de noviembre de 1969.

Organizaciones de la Sociedad Civil de Latinoamérica. “Declaración de Quito acerca de la exigibilidad y realización de los derechos económicos, sociales y culturales

(DESC) en América Latina y el Caribe", 24 de julio de 1998. http://www.derechos.org.ve/pw/wp-content/uploads/desc_01.pdf.

Parlamento Europeo. "Salud Mental en el mundo laboral digital", 5 de julio de 2022. https://www.europarl.europa.eu/doceo/document/TA-9-2022-0279_ES.pdf.

Parlamento Europeo, y Consejo Europeo. Reglamento General de Protección de Datos, L 119/1 § (2016).

Peralta-Díaz, Fabrizio. "Publicación | Feed | LinkedIn". Accedido 14 de junio de 2024. https://www.linkedin.com/feed/update/urn:li:activity:7204134049756430336/.

———. "Publicación | Feed | LinkedIn". *Linkedin*, 7 de agosto de 2024. https://www.linkedin.com/feed/update/urn:li:activity:7226964273808248832/.

———. "Publicación | Feed | LinkedIn". Accedido 14 de junio de 2024. https://www.linkedin.com/feed/update/urn:li:activity:7204134049756430336/.

———. "Publicación | LinkedIn". Accedido 23 de octubre de 2024. https://acortar.link/lssBeA.

———. "Publicación | LinkedIn". *Linkedin.com*. Accedido 12 de junio de 2024. https://www.linkedin.com/posts/peraltadiaz_el-23-de-abril-del-2024-ante-el-pleno-de-activity-7189652862111547392-ssA8/?utm_source=share&utm_medium=member_ios.

Primicias. "La salud mental de los niños en Ecuador está marcada por los contrastes". *Primicias*, 5 de julio de 2023. https://www.primicias.ec/noticias/sociedad/ninos-salud-mental-depresion-acoso/.

Ramírez, Diego Alonso García, y Santiago Giraldo Luque. "Presentación del número: la economía de la atención en un internet monopolizado". *Anuario Electrónico de Estudios en Comunicación Social "Disertaciones"* 15, n.º 2 (11 de julio de 2022). doi:10.12804/revistas.urosario.edu.co/disertaciones/a.11964.

Red Iberoamericana de Protección de Datos. Estándares de Protección de Datos Personales para los Estados Iberoamericanos (2017).

———.. "Historia de la Red Iberoamericana de Protección de Datos (RIPD) | Red Iberoamericana de Protección de datos". Accedido 8 de octubre de 2024. https://www.redipd.org/es/la-red/historia-de-la-red-iberoamericana-de-proteccion-de-datos-ripd.

———. "Países miembros", s.f. https://www.redipd.org/es/enlaces-de-interes/paises-miembros.

———. “Reglamento de la Red Iberoamericana de Protección de Datos”, 30 de noviembre de 2018. https://www.redipd.org/sites/default/files/2019-11/reglamento-ripd.pdf.

———. “Relación de entidades integrantes de la RIPD”. Accedido 8 de octubre de 2024. https://www.redipd.org/es/la-red/entidades-acreditadas.

———. “Se convirtió en Ley la aprobación del Convenio 108+ | Red Iberoamericana de Protección de datos”, 30 de noviembre de 2022. https://www.redipd.org/es/noticias/se-convirtio-en-ley-la-aprobacion-del-convenio-108.

Red Iberoamericana de Protección de datos. “Historia de la Red Iberoamericana de Protección de Datos”. *REDIPD*. Accedido 14 de junio de 2024. https://www.redipd.org/es/la-red/historia-de-la-red-iberoamericana-de-proteccion-de-datos-ripd.

Ríos Nicoli, Brian Martin. “Radicalización digital: el efecto de las redes sociales en el extremismo político y el discurso del odio”. *Ciencia Latina Revista Científica Multidisciplinar* 7, n.º 1 (23 de marzo de 2023): 10749-55. doi:10.37811/cl_rcm.v7i1.5247.

Roa, Mónica, y Klugman Barbara. “Considering strategic litigation as an advocacy tool: a case study of the defence of reproductive rights in Colombia”. Reproductive Health Matters 22, no 44 (enero de 2014): 31–41. doi:10.1016/S0968-8080(14)44804-3.

RSA. The Truth About Algorithms, 2018. https://www.youtube.com/watch?v=heQzqX35c9A.

Ruzzarin, Diego. “La inmediatez de las redes sociales y cómo nos afecta psicológicamente”, 2021. https://www.youtube.com/watch?v=ioAkdPKJPdo.

Sáenz, Arianna. “Publicación | Feed | LinkedIn”. Accedido 23 de agosto de 2024. https://www.linkedin.com/feed/update/urn:li:activity:7231455505955651584/.

Salao Sterckx, Emilio. “¿A qué edad los niños deben usar dispositivos digitales?” *Conexion PUCE*, 27 de mayo de 2022. https://conexion.puce.edu.ec/a-que-edad-los-ninos-deben-usar-dispositivos-digitales/.

SaludOnNet, Equipo Médico de. "¿Cómo afecta en la salud mental y física el uso excesivo de pantallas?" *Blog SaludOnNet*, 3 de octubre de 2024. https://www.saludonnet.com/blog/como-afecta-en-la-salud-mental-y-fisica-el-uso-excesivo-de-pantallas/.

Santiago Muñoz, Ana. "La sociedad de control: una mirada a la educación del siglo XXI desde Foucault". *Revista de filosofía* 73 (octubre de 2017): 317-36. doi:10.4067/S0718-43602017000100317.

Saura García, Carlos. "El lado oscuro de las GAFAM: monopolización de los datos y pérdida de privacidad". *Veritas*, n.º 52 (agosto de 2022): 9-27. doi:10.4067/S0718-92732022000200009.

SEMrush Blog. "¿Qué es el Big Data Marketing y qué ventajas ofrece?" Accedido 19 de noviembre de 2019. https://es.semrush.com/blog/que-es-big-data-marketing-ventajas/.

Suayed. "Análisis, diseño e implementación de algoritmos", 2017.

Superintendencia de Protección de Datos Personales. "Publicación | LinkedIn", 5 de noviembre de 2024. https://acortar.link/pId4vh.

Tecnología Educativa. "Infotecnología la Revolución Tecnológica: Concepto de Infotecnología". *Tecnología Educativa*. 19 de marzo de 2016. https://tecnologiaeducativawordpreescom.wordpress.com/2016/03/19/concepto-de-infotecnologia/.

Tejeda, H.A., T.S. Shippenberg, y R. Henriksson. "The dynorphin/kappa-opioid receptor system and its role in psychiatric disorders". *Cellular and Molecular Life Sciences* 77, n.º 5 (2020): 857-80.

Terán, Pablo. "Una empresa extrae datos de la retina de cientos de ecuatorianos posiblemente violando derechos de privacidad e información personal". *Fundamedios*, 31 de julio de 2024. https://www.fundamedios.org.ec/una-empresa-extrae-datos-de-la-retina-de-cientos-de-ecuatorianos-posiblemente-violando-derechos-de-privacidad-e-informacion-personal/.

Thai, Helen, Christopher G. Davis, Wardah Mahboob, Sabrina Perry, Alex Adams, y Gary S. Goldfield. "Reducing Social Media Use Improves Appearance and Weight Esteem in Youth with Emotional Distress." *Psychology of Popular Media* 13, n.º 1 (enero de 2024): 162-69. doi:10.1037/ppm0000460.

Think with Google. "Generación Y (millenials) y Z: características y diferencias". *Think with Google*. Accedido 2 de mayo de 2023. https://n9.cl/f2zz6.

Tribunal Europeo de Derechos Humanos. "Convenio Europeo de Derechos Humanos", 1950.

The Social Dilemma. "Digital Rights are Human Rights". Accedido 16 de septiembre de 2020. https://thedigitalrightsdilemma.splashthat.com.

Uhls, Yalda T., Minas Michikyan, Jordan Morris, Debra Garcia, Gary W. Small, Eleni Zgourou, y Patricia M. Greenfield. "Five days at outdoor education camp without screens improves preteen skills with nonverbal emotion cues". *Computers in Human Behavior* 39 (1 de octubre de 2014): 387-92. doi:10.1016/j.chb.2014.05.036.

*UNESCO*. "Crecer En La Era de Las Fake News"., Accedido 6 de abril de 2021. https://es.unesco.org/courier/2021-2/crecer-era-fake-news.

Unicef. "Aumenta la preocupación por el bienestar de los niños y los jóvenes ante el incremento del tiempo que pasan frente a las pantallas, según UNICEF", 4 de febrero de 2021. https://www.unicef.org/lac/comunicados-prensa/aumenta-la-preocupacion-por-el-bienestar-de-los-ninos-y-los-jovenes-ante-el-incremento-del-tiempo-frente-a-las-pantallas.

———. "Niños en un mundo Digital", 2017. www.unicef.org/SOWC2017.

———. "Cinco formas en que la pandemia impactó a los adolescentes", 2021. https://www.unicef.org/uruguay/crianza/adolescencia/cinco-formas-en-que-la-pandemia-impacto-los-adolescentes.

Unicef, y Ministerio de Educación. "Resultados de las encuestas de monitoreo del impacto de la pandemia de COVID-19 en la comunidad educativa ecuatoriana", 2022.https://www.unicef.org/ecuador/media/10156/file/Ecuador_encuestas_covid_educacion.pdf.pdf.

Velazco Rondón, David Licurgo. "La criminalización de la protesta social y el caso

Vistazo. "Proyecto de ley de protección de datos personales pasa primer debate en el Legislativo". Accedido 2 de abril de 2021. https://n9.cl/j9jf6o.

*VASM- Superintendente sin Superintendencia.*, 2024. https://www.youtube.com/watch?v=f7Bk4Jf-3QE.

Ventura Robles, Manuel. "El Sistema Interamericano de Protección de los Derechos Humanos". En *Los sistemas internacionales de protección de los derechos humanos*, 1.ª ed. Universidad del Externado de Colombia, 2014. doi:10.2307/j.ctv13vdg3r.

Velazco, David, y Rosa Quedena. La criminalización de la protesta social y el caso Majaz. Primera edición. Lima: Fedepaz/Oxfam, 2015.

Villán Durán, Carlos. "Manual sobre el sistema universal de protección de los derechos humanos", 2016. https://n9.cl/hxv5cf.

VPRO Documental. “Shoshana Zuboff sobre el capitalismo de vigilancia”, 2019. https://www.youtube.com/watch?v=hIXhnWUmMvw&feature=youtu.be.

Warnken, Diego Nicolás Castillo. “Caracterización y predicción de conducta de usuarios de aplicación móvil enfocado a proceso “on boarding” utilizando herramientas de Machine Learning”, 2022.

World Vision. “Salud mental en niños, niñas y adolescentes en Ecuador: 7 de cada 10 se sienten felices, pero el 20% enfrenta dificultades para identificar tristeza y estrés”. Accedido 29 de abril de 2025. https://worldvisionamericalatina.org/ec/sala-de-prensa/salud-mental-en-ninos-ninas-y-adolescentes-en-ecuador-7-de-cada-10-se-sienten-felices-pero-el-20-enfrenta-dificultades-para-identificar-tristeza-y-estres.

World Vision, Ministerio de Educación, y Red Nacional de Niñas, Niños, Adolescentes y Jóvenes Wamprakunapak Yuyaykuna. «Segunda Encuesta Nacional: “Tu voz, tus derechos”. Sobre salud mental de niñas, niños, adolescentes y jóvenes», 2023. https://worldvisionamericalatina.org/ec/sala-de-prensa/salud-mental-en-ninos-ninas-y-adolescentes-en-ecuador-7-de-cada-10-se-sienten-felices-pero-el-20-enfrenta-dificultades-para-identificar-tristeza-y-estres.

“¡Worldcoin Está En Ecuador!” Accedido 15 de agosto de 2024. https://worldcoin.org/holaecuador.

X (formerly Twitter). “APC (APC_News) / X”, 5 de junio de 2024. https://x.com/apc_news.

# Anexos

## Anexo 1: Formulario de Consentimiento Informado

**Título de la investigación:**
Estudio de situación sobre la explotación económica de datos personales en redes sociales y su impacto en el derecho a la salud mental de niños, niñas y adolescentes en el Ecuador.

**Investigador:**
Víctor Daniel Espinosa Mogrovejo

**Tutor:**
Luis Fernando Enríquez Álvarez

**Institución:**
Universidad Andina Simón Bolívar, sede Ecuador

**Propósito de la investigación:**
El propósito de esta investigación es analizar la explotación económica de datos personales en redes sociales y su impacto en la salud mental de niños, niñas y adolescentes en Ecuador, con el fin de identificar problemáticas y proponer soluciones desde la exigibilidad de derechos.

**Propósito de la entrevista:**
La entrevista busca recopilar información y opiniones de expertos y usuarios para complementar el análisis del estado de situación, considerando perspectivas profesionales y experiencias directas sobre la protección de datos personales y sus implicaciones en la salud mental.

**Confidencialidad:**
Toda la información proporcionada será tratada con estricta confidencialidad. Los datos personales del entrevistado no serán divulgados en el informe de investigación ni en ninguna publicación derivada, a menos que el entrevistado autorice expresamente su inclusión.

**Voluntariedad:**
La participación en esta entrevista es completamente voluntaria. El entrevistado tiene el derecho de retirar su consentimiento y finalizar su participación en cualquier momento, sin que esto implique consecuencias negativas.

**Duración:**
La entrevista tendrá una duración aproximada de 45 a 60 minutos.

**Uso de la información:**
La información recopilada será utilizada exclusivamente para fines académicos, como parte del informe de investigación requerido para el proceso de graduación en la Universidad Andina Simón Bolívar.

**Consentimiento:**
Declaro que he sido informado/a sobre los objetivos y alcances de esta entrevista, y comprendo mis derechos como participante. Acepto participar de manera voluntaria en la entrevista y autorizo el uso de la información proporcionada de acuerdo con los términos descritos en este formulario.

**Firma del entrevistado/a:**
Nombre completo: _____
Firma: _____ Fecha: _____

**Firma del investigador:**
Víctor Daniel Espinosa Mogrovejo
Firma: _____ Fecha: _____

**Anexo 2: Cuadro de Entrevistados**

| Nº | Nombre del entrevistado | Profesión | Experiencia profesional |
|---|---|---|---|
| **1** | Emilio Salao | Psicólogo Clínico y Docente Universitario | Salud mental infantil y adolescente, docencia universitaria. |
| **2** | Emilia Piedra | Psicóloga Infantil y Educativa | Psicología infantil en entornos clínicos y educativos. |
| **3** | Fernando Ocaña | Psicólogo Educativo y Coordinador DECE | Salud mental educativa, prevención de violencia escolar. |
| **4** | Henry Zaruma | Psicólogo Clínico y Comunitario | Intervención comunitaria, enfoque en género e infancia. |
| **5** | Lorena Naranjo | Abogada | Exdirectora de DINARDAP, autora de política pública sobre Internet segura. |
| **6** | Paulina Casares Subía | Docente universitaria | Educación en derechos digitales y protección infantil. |
| **7** | Ola Bini | Programador y activista | Especialista en privacidad y ciberseguridad. |
| **8** | Santiago Acurio | Psicólogo Clínico y Docente Universitario | Datos personales y derechos de infancia. |
| **9** | Patricia[485] | Usuaria de tecnología | Experiencia personal con *Worldcoin* y tratamiento de datos biométricos. |

[485] Seudónimo para garantizar el anonimato

**Anexo 3: Cuestionario de Preguntas**

**Preguntas realizadas a las personas expertas en protección de datos personales:**

| N° | Preguntas |
|---|---|
| **1** | ¿Cuáles son los principales riesgos para la privacidad y la protección de datos personales de los niños, niñas y adolescentes en Internet y las redes sociales? |
| **2** | ¿Existen normativas o políticas que garanticen la protección de datos personales y la privacidad de niños, niñas y adolescentes en redes sociales e Internet? |
| **3** | ¿Considera que el modelo de negocio de las empresas de Internet y redes sociales promueven la vulneración a la protección de datos personales de niños, niñas y adolescentes? |
| **4** | ¿Qué estrategias pueden implementar los padres en el hogar para promover una relación saludable y segura con la tecnología, protegiendo así la privacidad y la salud mental de sus hijos? |
| **5** | ¿Qué podría hacer el Estado para garantizar el derecho a la protección de datos personales de niños, niñas y adolescentes? |
| **6** | ¿Cómo pueden las empresas de tecnología y redes sociales ajustar sus políticas y prácticas para garantizar la protección de los datos personales y la salud mental de los niños y adolescentes? |
| **7** | ¿Qué podrían hacer las organizaciones de la sociedad civil para promover la protección de los datos personales de los niños, niñas y adolescentes en redes sociales e internet? |

**Preguntas realizadas a las personas expertas en Salud Mental en el Entorno Digital**

| N° | Pregunta |
|---|---|
| **1** | ¿Qué cambios ha observado en el comportamiento de los niños y niñas con el aumento del uso de las Internet y redes sociales en los últimos años? |
| **2** | ¿Qué tipos de problemas de salud mental ha visto asociados con el uso del Internet y redes sociales en niños y niñas? |
| **3** | ¿Ha observado alguna relación entre el tiempo que pasan los niños y niñas en Internet y redes sociales y su bienestar emocional? |
| **4** | ¿Qué impacto cree que tienen las estrategias de diseño de redes sociales, como las notificaciones constantes y la gamificación, en la salud mental de los niños y niñas? |
| **5** | ¿Ha notado diferencias en cómo los niños y niñas reaccionan emocionalmente a las interacciones en línea en comparación con las interacciones cara a cara? ¿Qué importancia tienen las interacciones sociales en persona para el desarrollo de habilidades sociales y emocionales en los niños y niñas en la era digital? |
| **6** | ¿Cree que existe una relación entre el modelo de negocio de Internet y redes sociales y el aumento de los problemas de salud mental en niños y niñas? |
| **7** | ¿Qué recomendaciones daría a los padres y educadores para abordar los riesgos para la salud mental asociados con el uso de Internet y redes sociales por parte de los niños y niñas? |
| **8** | ¿Qué papel cree que deberían desempeñar las empresas de redes sociales y las autoridades gubernamentales para mitigar los impactos negativos en la salud mental de los niños y niñas? |
| **9** | ¿Qué podría hacerse desde la sociedad civil para prevenir y abordar estos problemas? |

**Preguntas realizadas a Patricia**[486]

| N° | Pregunta |
|---|---|
| **1** | ¿Cuál es su nombre? |
| **2** | ¿De dónde es y cuántos años tiene? |
| **3** | ¿Cuál ha sido su experiencia con Worldcoin y cómo se enteró de él? |
| **4** | ¿Se enteró de Worldcoin porque le dijeron a sus compañeros del trabajo? ¿Qué le dijeron sus compañeros? |
| **5** | ¿Por qué le dijeron que se registrara? |
| **6** | ¿Cómo le pagaban, en efectivo? |
| **7** | ¿Qué son los tokens que mencionó? ¿Cómo funciona el proceso de venta de los mismos? |
| **8** | Después de registrarse, ¿cambió su opinión sobre Worldcoin? ¿Qué ocurrió después de descargar la aplicación? |
| **9** | ¿Le dijeron para qué se recopilaba su información? |
| **10** | ¿Le leyeron algún acuerdo o firmó algún contrato? |
| **11** | ¿Sabe para qué se va a utilizar su información? |
| **12** | ¿Cómo se siente ahora respecto a su participación en Worldcoin? |
| **13** | ¿Conoce a quién podría reclamar por este tipo de tratamientos? |
| **14** | ¿Podría obtener efectivo de las monedas de Worldcoin? ¿Cómo podría transformar Worldcoins en dólares o efectivo? |

[486] Seudónimo para garantizar su anonimato.

## Anexo 4: Entrevistas

### Emilio Salao[487]

1. ¿Ha existido, desde tu punto de vista como psicólogo, un aumento en los problemas de salud mental en los niños y niñas actualmente?

Yo creo que un punto clave para reflexionar sobre los aspectos psicosociales de la niñez y la adolescencia se debe situar en, no sé si abordar propiamente en la psicología hablar de problemas es cuando normalmente hemos hecho un proceso de identificación diagnóstico, en donde ya hemos hecho también una recolección de lo que implica el estado o la vida de una persona y a partir de eso se identifican problemáticas, pero normalmente lo que si se presenta y se ha visto que si ha crecido han sido las preocupaciones, o como también en psicología clínica se lo denomina "las demandas de atención". La "demanda de atención" se refiere, en otras palabras, a las necesidades que presentan adultos, instituciones educativas respecto a lo que está pasando con niños y niñas. No nos olvidemos que, en el Ecuador como en otros países del mundo, la Ley Orgánica de Salud Mental estipula que: toda persona menor de edad debe llegar bajo autorización, debe ser atendida bajo autorización de sus tutores legales, entonces normalmente lo que sucede es que quienes solicitan la atención son los tutores legales a veces de manera directa o porque ha sido una recomendación de la unidad educativa, u otra instancia de la salud, en fin.

Entonces si se van presentando preocupaciones que han cambiado con el tiempo, y un punto clave que si marca la diferencia de eso es precisamente la pandemia del COVID-19. Antes de la pandemia había unas necesidades específicas que eran muy notorias en el espacio de consulta y después de la pandemia se presentaron otras, o se retoman esas mismas demandas, pero ya con otros elementos importantes que si invitan a la reflexión.

La pandemia marcó preocupaciones que empiezan a distinguirse o que son diferentes a las que existía antes de la pandemia. En general en el país la necesidad de servicios de salud mental aumentó a partir de la pandemia del COVID-19, pero sobre todo en los primeros meses de las normas restrictivas de contacto que se estableció en el decreto d17 de la presidencia de la república. A partir de eso si hubo mayor demanda, pero fue una demanda que creció en términos poblacionales, es decir, no solo era de niñez, sino también de adolescentes, adultos y adultos mayores también. Después, cuando empiezan las normas de relajación en el contacto después de los tres, cuatro primeros meses de la pandemia, como que disminuye un poco también el tema del volumen de solicitudes de atención. Sin embargo, si se van posicionando algunas necesidades específicas de la salud mental que son notorias hasta ahora que tienen que ver con: las relaciones familiares, sobre todo en los niños que tiene mucho que ver con los vínculos con sus padres; el desgaste psicológico que provocó la Tele Educación en la población de niñez y adolescencia, sobre todo porque la Tele Educación implicó un tema muy acelerado de las dinámicas educativas que no son solamente formativas, sino que también tienen y guardan una profunda relación con las necesidades psicosociales de cada etapa de la vida. Entonces hubo impactos en ese sentido también.

Por lo que, siempre que se trata de hablar sobre la situación de la niñez y adolescencia en el Ecuador no se puede dejar de lado el tema de la pandemia porque si marca un antes y un después sobre la salud mental de la población más joven del Ecuador.

---

[487] Psicólogo clínico, terapeuta y coordinador de vinculación con la colectividad del Instituto de Salud Pública de la Pontificia Universidad Católica del Ecuador. Entrevistado el 10 de mayo de 2024.

2. ¿Existen más demandas con respecto a problemas derivados de la tecnología, de dispositivos tecnológicos en niños, niñas y adolescentes?

No existe ninguna estadística que señale eso, en general porque no hay estudios nacionales sobre salud mental, en donde a nivel estadístico te puedan mostrar primero cuáles son las problemáticas de salud mental más frecuentes o los trastornos mentales de prioridad de atención, tampoco hay estadísticas confiables nacionales que nos hablen respecto al tema de accesibilidad a los servicios de salud mental. Hay algunos estudios más específicos por supuesto, pero tu pregunta exigiría que exista un estudio de ese nivel que no existe. Entonces no se puede saber si es que existen más demandas a nivel nacional sobre atención para niños por temas relacionados a la digitalidad.

Desde la impresión que puedan tener colegas, normalmente desde espacios que suelen llamarse estudios de casos, también espacios donde se reflexiona de la psiquiatría infantil y también la psiquiatría alrededor de niños, niñas y adolescentes puede haber y puede presentarse también como preocupaciones específicas que tiene que ver con la relación en espacios digitales o los usos digitales, sí, si se presentan, pero no se podría afirmar así con toda certeza si hubo un aumento de esas temáticas como solicitud a nivel nacional. No hay un estudio que lo pruebe. Si se presenta eso ¿no?, más digamos en la consulta, pero no por eso quiere decir que es representativo a nivel nacional.

3. ¿Cuáles son los principales desafíos que enfrentan los niños y niñas en términos de salud mental debido al uso de internet y redes sociales? ¿qué tipos de problemas de salud mental se encuentran asociados al internet (posibles adicciones, etc.)? ¿qué tipos de problemas pueden enfrentar los niños en espacios digitales?

Normalmente los problemas de abordaje que se tiene con respecto a los impactos y los efectos a la digitalidad en nuestras vidas suele entenderse o abordarse en la búsqueda de la normalidad, sin embargo creo que siempre es importante hablar de las problemáticas presentes en la normalidad antes que las anormalidades en sí. Lo que podríamos entender lo patológico, es decir, no todas las problemáticas caen en lo que entenderíamos como trastornos o problemáticas de salud mental pero ya la misma cotidianidad de los consumos digitales, ya planteaban algunos problemas que normalmente no se reflexionan. Y es que depende mucho desde donde se enfoque el abordaje de la relación sujetos-tecnología, o sujetos-espacios digitales. Por ejemplo, cuando se hablaba sobre el bom del internet a mediados de los 90's en el mundo, cuando se hablaba de los espacios digitales, se hablaba como un espacio virtual, entonces el concepto de vida era muy antiguo y siempre refería a que la realidad es una cosa y que lo que se establece o lo que se hace, las actividades que se tienen, en el internet son distantes a la realidad, pero desde los 2000´s al 2010 se habló de otro concepto que era "Cyberespacio" que mantenía el mismo principio de que una cosa es realidad y otra cosa son los espacios de internet, pero que la idea del "Cyberespacio" expande el concepto desde este otro lugar que existe en la cultura, pero todavía se apega a que es un lugar irreal.

Más bien el crecimiento y el desarrollo de las redes sociales a partir del 2008 en adelante, ahí si empieza a cuestionarse si realmente podemos llamar "Cyberespacio" o "Virtual" a estos otros lugares de relación. Entonces como las redes sociales botan las plataformas. Pero a partir del 2018, 2017, se introduce un nuevo concepto que es la idea de la realidad mediada porque aparecen nuevas tecnologías que lo que hacen es esto de la realidad aumentada, es decir, que las personas están en un espacio real a través de cosas muy lúdicas o cosas académicas, o laborales, tienen interacciones con la realidad que ya involucran dispositivos conectados al internet. Y esto también afecta bastante a ciertos espacios, sobre todo a los espacios educativos, donde están

presentes los niños. Así que en ese tema de la realidad mediada si hay unas problemáticas pero no las llamaríamos trastornos ni problemas de salud mental, pero si hay problemáticas que preocupan: uno es que las dinámicas de interacción que producen las realidades mediadas son de estímulo-respuesta, es decir que si alguien pone un contenido se da reacción a ese contenido sobre todo en redes sociales, y esa es la dinámica de contacto, lo que produce esto es que las personas conforme van creciendo a partir de por ejemplo los 8-9 años vayan presentando conductas de mayor impulsividad, pero no quiere decir trastornos de déficit de atención o agresividad ni nada de eso que normalmente se le ubica ya más cercano a la idea del trastorno, sino que en la realidad, en la vida cotidiana, en la interacción social cotidiana se muestra una aproximidad mayor a la impulsividad, pero no es un problema de salud mental la impulsividad, más bien es una característica, una cualidad de las personas, un rasgo, podríamos llamarlo así.

Por eso me parece que es importante primero citar los problemas de la normalidad o de lo cotidiano antes que los trastornos porque ese es uno de los efectos principales, es decir para el desarrollo del pensamiento y la relación social necesitamos vivir tres momentos todos los seres humanos: uno es la percepción, luego la elaboración y después la respuesta. Las dinámicas del consumo digital se saltan el paso del medio, entonces por eso solo pasamos de estímulo a respuesta. Cuando pensamos en adultos que nacieron por ejemplo en la década de los 70´s o los 80's del sigo XX, esos adultos tuvieron un tiempo incluso neurológico de desarrollo que, a pesar de que podrían ser hartos consumidores de la digitalidad, no presentan estas problemáticas de impulsividad, pero ¿qué significa para una persona nacida en la época de los 2010? Empezar con su vida ya con hábitos digitales desde el principio, que implica esto en su desarrollo neurológico en general, en sus interacciones también sociales. Entonces por eso siempre se debe diferenciar entre los más vulnerables en el caso de los niños, es que los niños nacen en este contexto, lo cual implica que es un contexto que determina mucho cual va a ser su desarrollo precisamente porque los hábitos digitales están cada vez más pronto en la vida del niño. Así que encontramos niños de 2 años que ya tienen acceso a Smartphones, tal vez no son propietarios directos de un Smartphone pero si tienen actividades en el mismo. También nos encontramos con niños en edad escolar que tienen ya amplios usos digitales, sobre todo por el uso de videojuegos, redes sociales y chats. Por lo general lo que estamos observando es que tienen un consumo ya más pronto, más joven, más rápidamente se involucran en los espacios digitales. Normalmente esto suele ser asociado a la maternidad o a la paternidad. De hecho la parentalidad suele ser señalado a esto como un problema, pero en realidad creo que las empresas que son responsables del desarrollo de la tecnología toman la opción barata que es culpar a los padres por darles acceso inmediato, muy pronto, a sus hijos, cuando en realidad los sistemas cada vez están más involucrados y obligan de cierta manera, a que los padres tengan que permitir o darles acceso a gadgets a sus propios hijos porque son necesidades que se vinculan a lo cotidiano.

4. ¿Cómo equilibrar el derecho a usar la tecnología considerando lo necesario que es hoy en día y cómo evitar estos riesgos que vienen con ello, usar este tipo de tecnología?

Por ejemplo con el aumento de la inseguridad en el Ecuador en los últimos tres años, lo que se ha producido muchísimo es que padres están dando más pronto smartphones para poder mantener o usar estas aplicaciones donde pueden saber dónde están ubicados geográficamente (es la geoubicación), entonces sus hijos pasan con el sistema abierto geoubicación todo el tiempo, y no solo niños pequeños, también adolescentes. Entonces normalmente lo que esto genera en las relaciones parentales o en las relaciones familiares, es el aumento del control y la vigilancia como una dinámica propia de lo familiar y eso tiene un impacto psicosocial muy profundo en los niños.

Ahora bien Elisabeth Roudinesco habla, por ejemplo, de la omnipresencia de los padres en la vida de sus hijos precisamente por la incorporación de la gadget. De hecho, el concepto que ella utilizaba mucho era el del "Arcangel", que los padres dejan de ser padres y se vuelven arcángeles que están en permanente cuidado y vigilancia de sus hijos a través de smartphones, y ese concepto luego fue tomado hasta por una serie de televisión que se llama "Black Mirror" y produjo un capítulo sobre eso, pero es como uno de los elementos claves, no es anormalía, no está dentro del tema de trastornos, pero si está dentro de lo que normalmente entendemos lo cotidiano de una vida familiar, y analizar esos impactos sobre la cultura de la vigilancia entre ciudadanos, luego entre miembros de la familia, lo que produce es una dinámica psicosocial de desconfianza. Entonces no vas a escuchar nunca a un padre o a una madre que vive en la hipervigilancia de sus hijos, que se sienta tranquilo con esa hipervigilancia, ni a hijos que se sientan seguros con esa hipervigilancia. Lo que se construye es una dinámica de desconfianza.

En el libro de Shoshana Zuboff "Capitalismo de la Vigilancia" habla de cómo la vigilancia se traslada a la vida cotidiana, es decir antes necesitabas a la CIA, a los sistemas de inteligencia, pero ahora los ciudadanos se vuelven a sí mismos agentes de vigilancia sobre los otros, y cuando se piensa en eso en el marco familiar ¿Qué implicaría que se construyan dinámicas de vigilancia entre padres e hijos? Por ejemplo, o ahí se pone en juego precisamente la dificultad de construir relaciones vinculares optimas con otros. Los seremos humanos aprenden a hacer vínculos en sus núcleos familiares. Si esas capacidades de poder construir vínculos familiares son bloqueadas por estas dinámicas, lo que produce es que en el futuro tendrán dificultades también para generar otro tipo de vínculos propios de la vida adulta. Entonces estos son los impactos que no se pueden ver a corto plazo pero que, si se podrá ver en los adultos del 2030 al 2050, hay que preguntarse cómo será.

5. El contexto cambiante es uno de los desafíos, ya que, si bien no pueden llegar a entenderse como trastornos, si se pueden entender como problemas cuyas consecuencias las veremos en un tiempo todavía, sería más o menos los desafíos que tu identificas, ¿verdad?

Ya hay efectos ahora, por ejemplo, una cosa es el impacto, otra el efecto, pero ya hay efectos en este momento que es precisamente las dificultades vinculares entre padres e hijos. Ese es uno de los puntos que más aparece en las problemáticas ya propiamente trabajadas, es decir dificultades de los hijos que no se sienten en suficiente relación de confianza con sus padres y madres que viven relaciones también complejas con sus hijos basadas también mucho en cómo se proyectan sus propios fantasmas e inseguridades, puesto que perciben que sus hijos viven en mundos más vulnerables al mismo tiempo que los vigilan más. Creo que siempre es importante con la reflexión de niños hablar precisamente del desarrollo vincular y cómo esto se puede comprometer a lo largo de su vida. Yo lo pondría como uno de los aspectos nucleares.

6. ¿Qué importancia tienen las intervenciones sociales en persona para el desarrollo de habilidades sociales y emocionales en los niños y niñas en la era digital?

El tema de los problemas no solo está en relación al acceso sino también a la falta de acceso. Por ejemplo, entre mayor capacidad tiene un niño de acceder a una conectividad de internet en casa, tiene más oportunidades educativas, mientras que cuando vemos otros contextos del mismo territorio ecuatoriano, en donde existen problemas de conectividad, o la economía familiar no da suficiente como para tener internet en casa o que la institución educativa donde estudian no tiene conectividad, ahí se van estableciendo unas nuevas brechas sociales. Entonces la cuestión alrededor de la accesibilidad al internet es que lo que instituye son nuevas brechas

sociales, no solamente brechas de acceso al internet. Así que ahora vemos enormes diferencias en la calidad educativa entre niños de sectores donde existe mayor acceso al internet de otros que no. Normalmente el internet es un capital social tanto para un niño que tiene todos los accesos y gadgets a su disposición, como para aquel que no tiene ni siquiera un teléfono celular en la familia. Entonces en ambos casos es valorado, es bien reconocido, el acceso al internet como un elemento positivo, pero hay enormes brechas de acceso en nuestro país con respecto al internet que lo que primero producen son más brechas sociales basadas en las brechas educativas, en las brechas socioeconómicas. Como ha dicho Alba de la Selva es que las brechas del internet lo que muestran son las nuevas desigualdades del siglo XXI. Esa es una y muy importante.

Normalmente es en la etapa de la adolescencia en donde los chicos en el proceso de la configuración de la identidad perciben mucho más las diferencias de clases sociales. Entonces, pensando en un sentido proyectivo lo que vamos a ver siempre es que estas brechas de acceso lo que producen es mayores dificultades en la construcción de comunidad, en la construcción de lazos sociales más abiertos y diversos, que curiosamente es el espíritu contrario del internet, porque el internet supuestamente está colocado en el mundo para que nos podamos conectar entre todos, para que podamos liberar la información y tener acceso en igual de condiciones a todos, pero en realidad lo que observamos es que el internet en realidad promueve con estas brechas de acceso es una mayor desigualdad, y esto se traduce en las relaciones sociales entre niños, niñas y adolescentes. Esas brechas de acceso en la infancia son vistas simplemente como privaciones, luego se relacionan de manera más directa con el sentido de la aceptación social, con la inclusión social y la participación social. Los niños que no tienen ahorita internet probablemente en el futuro van a tener menos capacidad de participación social, menos acceso a la información y por ende tal vez menos oportunidades.

7. ¿Qué riesgos habría con el acceso al internet?

La capitalización simbólica del internet lo que produce es que para quienes no tienen suficiente acceso al internet, al momento de tener acceso, básicamente se enfocan mucho, sobre todo, al uso de las redes sociales. Por ejemplo, en la Universidad de Luzán, de Suiza, justamente hay docente de la facultad de economía de la PUCE que está haciendo su doctorado allá, y él hizo un estudio bastante interesante sobre el uso de redes sociales en niños, niñas y adolescentes suizos en la Universidad de Luzán, es en donde existe la población más baja uso de redes sociales, es decir casi no tienen cuentas en redes sociales, casi no usan el internet para tener cuentas en plataformas como Instagram, tik tok. Entonces, ciertos espacios en donde existe mayor desarrollo y donde existe más acceso hay menos uso de redes sociales. Mientras que, en donde existe más privación de acceso al internet, el poco acceso al internet se lo utiliza sobre todo para redes sociales.

Esto no significa que ser pobre es utilizar redes sociales, pero significa que normalmente alrededor del acceso al internet hay otra brecha, que no solamente es la brecha de acceso a la conectividad y a los aparatos sino también al uso. Entonces la brecha de uso lo que determina es que haya unos usos más desarrollados para quienes más posibilidades de conectividad y unos usos menos desarrollados para quienes tienen menos conectividad, y en este sentido las plataformas de redes sociales son las que menos capacidad de uso necesitan del usuario para poder utilizar las redes sociales. De esta forma observamos más niños, niñas y adolescentes de lugares en donde existe poca accesibilidad que si tienen redes sociales, pero no dan otros usos tampoco a las oportunidades que podría tener el internet. El impacto que esto tiene directamente sobre la vida psíquica es que hay menos elementos de por medio que le permitan filtrar cuál es el impacto que

tiene su vida al mirar una estética corporal en Instagram, al mirar un estilo de vida en una red social que no puede reproducir, entonces produce una profunda insatisfacción consigo mismo.

8. ¿Cómo afecta el acceso al internet sobre la percepción del mundo y de sí mismos en los niños, niñas y adolescentes? ¿Estas imágenes, mensajes en redes sociales pueden impactar en la autoestima y la imagen corporal de los niños y niñas?

Es un riesgo. La cuestión es siempre considerar que el tema de la infancia y más tarde el de la adolescencia, sobre todo la adolescencia, el tema de la construcción de la identidad es un proceso, entonces mucho de lo que implica la construcción de la identidad viene por la absorción sobre las cosas que están presentes en la cultura vigente. El acceso muy temprano, sobre todo a redes sociales, lo que produce es que precisamente esa observación de los contenidos es considerada la realidad. El hecho de que pensadores hayan hablado de la realidad mediada, es porque ya no se la puede distinguir de la otra realidad; de la realidad de los objetos concretos. En ese sentido es que esa se considera la realidad y lo que sucede es que hay una distancia o brecha entre la capacidad de reproducir esos mismos niveles de vida o de ti. Normalmente lo que lleva a tener este problema es consigo mismo. En la niñez se observa, como cada vez más también hay un inicio más pronto de la adolescencia, esto se debe al uso acelerado de redes sociales, especialmente de redes sociales, y ahí la idea sería relacionar más como el inicio temprano de la adolescencia tiene la necesidad de una mayor maduración del cuerpo. Esto implica que hay menos tiempo para la experiencia de la niñez y hay una necesidad de crecer más rápido para alcanzar esos estándares estéticos.

En la niñez es necesario vivir al menos unas dos a tres etapas de la vida, sobre todo lo que implica el desarrollo psicosexual y más bien esta aceleración lo que produce es que disminuya en el tiempo la experiencia de cada etapa, especialmente la etapa de latencia que sucede más o menos entre los 5 y 9 años, en donde hay una experiencia mucho más placentera sobre de la propia niñez, porque de los 0 a los 5 años vivimos otras cosas, pero esa etapa de latencia se ha reducido. Ahora estamos encontrándonos con que hay unos inicios de la etapa de la pre adolescencia mucho más temprano que acortan el período de la niñez, diferenciando infancia de niñez (infancia es hasta los 5 años y niñez desde los 5 años en adelante por lo que se acorta sobre todo el período de la niñez).

El mismo ciclo de vida hace que las personas atraviesen esas etapas a menos que realmente una problemática profunda, como por ejemplo una discapacidad mental, sí eso puede suceder, pero las etapas del desarrollo psicosexual nunca son completadas a la perfección, siempre quedan cosas irresueltas en cada etapa, y eso es lo que configura el aspecto particular de la personalidad, pero la aceleración lo que puede promover es otro tipo de problemáticas complejas también precisamente porque no hay un tiempo psicológico, un tiempo psíquico adecuado para poder madurar en cada etapa. Cada etapa tiene sus propios niveles de maduración, pero si no se pueden, por el mismo tema del crecimiento, resolver en cierta medida consistente probablemente esto puede desencadenar en otras problemáticas en la adolescencia.

Normalmente la cuestión que vivimos con las preocupaciones sobre los usos digitales y la infancia es que muchas de estas problemáticas son proyectivas, entonces ¿qué es lo que va a pasar más adelante? Más allá del comportamiento de un niño, más allá de las cosas o contenidos que consuma, es la dinámica de relación que esto produce con su propio cuerpo, que produce con los demás, con el ambiente familiar, y eso es lo que se debe analizar más adelante.

Hay ciertos fenómenos culturales en donde se posiciona también la experiencia del cuerpo de la niñez y de la adolescencia desde ya otros lugares mucho más adultos, por ejemplo, el tema d ela sexualización de los niños a través de las plataformas de redes sociales. Esto lo que incorpora

es que el cuerpo que se proyecta en las redes sociales no es el cuerpo que un niño pueda tener a esas edades. La cuestión es que al ser la idea de la edad y de la maduración sobre todo un concepto cultural, si se impacta con un cuerpo que es real y que si tiene un funcionamiento biológico y que también tiene un tiempo biológico. Empiezan a diferenciarse de manera importante los propios pasos del desarrollo del ciclo de vida y lo que la cultura empieza a imponer o a instaurar como lo propio, lo ético, lo estético, lo esperado de un cuerpo de un niño, de un adolescente de un adulto.

9. ¿Qué impacto crees que tienen las estrategias de diseño de las redes sociales como las notificaciones constantes?

Creo que un poco lo respondí con estos comentarios sobre cómo se basan mucho en la lógica de estímulo respuesta, y ese es el aspecto más central de la dinámica cognitiva que se establece en el contacto con redes sociales, es decir, no es propiamente un espacio donde se evalúa, se aprecia, se construye una opinión sobre el contenido sino solo se reacciona al contenido. Lo que produce precisamente es reactividad.

10. ¿Has observado alguna diferencia en la forma como los niños, niñas y adolescentes interactúan en línea en comparación con como lo hacen de manera personal?

No propiamente fuera de los espacios de investigación en metodologías educativas cómo es esto de las tablets en el aula y cuestiones así, pero no tendría mucho que decir ahí al respecto. No he observado de manera directa.

En general, no solo con niños y niñas es esto que Elizabeth Roudinesco dice que es la soberanía del yo, y es que lo que promueve el uso de redes sociales es a tener una amplia conectividad con muchas personas pero cada vez más individualizado, entonces lo que promueve muchísimo el uso de redes sociales es la individualización. Esto pone por prioridad el bienestar, satisfacción o placer personal por sobre las responsabilidades y la correspondencia con los otros. Te conecta al mismo tiempo con los otros y contradictoriamente lo que hace es individualizarte más. Esto, en la experiencia de la niñez lo que puede producir es menos relaciones responsables.

11. ¿Qué recomendaciones darías a los padres y educadores para abordar los riesgos para la salud mental asociados con el uso de internet y redes sociales para los niños y niñas?

La recomendación es que puedan exigir las instituciones que son responsables del control del contenido en el Ecuador, que puedan realmente promulgar cómo mecanismos que permitan que los niños al mismo tiempo tengan menos acceso a contenidos problemáticos o para adultos, que la puerta hacia la plataforma de redes sociales en el Ecuador no estén tan abiertas, que se empiece a legislar más alrededor de eso porque responsabilizar a los padres y a los educadores de las escuelas sobre eso implica que ellos tengan, como David y Goliat, enfrentar a un monstruo gigantesco. Más bien lo que puede promover más ahora es precisamente que las instituciones educativas y las familias, la sociedad, exija más de su estado el control sobre la presencia de este tipo de plataformas en nuestra realidad.

Que esas cosas si se ven en otros países, como por ejemplo en Alemania, o en países europeos, en donde hay verdaderamente una serie de pasos que hace que haya menos invasión de las redes sociales en la vida de los niños, niñas y adolescentes, y, aun así, es muy fuerte la presencia de redes sociales. Pero nosotros si tenemos las puertas abiertas de par en par y eso es peligroso. Recomiendo una movilización social.

12. ¿Qué papel deberían desempeñar las empresas de redes para mitigar estos impactos en la salud mental de niños y niñas?

Me parece que las legislaciones de los estados, especialmente de países latinoamericanos como el Ecuador, puedan poner por encima de los intereses económicos de estas empresas las leyes con las que regulan las relaciones con sus ciudadanos, sea la prioridad. Entonces a una empresa no se le puede pedir tomar sensibilidad sobre las necesidades de una población o las prioridades de salud pública porque no lo van a hacer. Pero creo que en las normas nacionales e internacionales se les dé más autoridad a los países para poder controlar y pedir que rindan cuentas estas organizaciones por las acciones de sus países.

Eso es clave. Nuestro país no tiene ningún tipo de regulación en ese sentido fuera de los aspectos formales de la Dinardap y cosas así, que son muy puntuales, pero en realidad me parece que son más formalidades y que no se rinden cuentas ante el estado ecuatoriano.

Que quieran empresas o plataformas internacionales desarrollar actividades económicas en el Ecuador es legítimo, pero la cuestión es que se puedan construir parámetros que regulen esas actividades y que también pongan sanciones y exijan la rendición de cuentas sobre esas actividades en nuestro medio que influencian en cosas que tú has dicho como el tema del efecto sobre las democracias, los consumos, los impactos en la niñez. Entonces sí, las empresas tienen responsabilidades que hay que exigir que cumplan, pero para eso se necesitan instrumentos que nos permitan exigir eso.

13. ¿Qué podría hacer el estado para garantizar el derecho a la salud mental de los niños, niñas y adolescentes en temas digitales?

Que dentro de lo que implica esto de la problemática de salud pública en el sentido de que hay unos determinantes que fomentan una serie de fenómenos, es que las preocupaciones sobre el impacto de la digitalidad en la vida pasen a ser prioridades a tratar, por ejemplo, en la promoción de la salud y la prevención también de trastornos mentales u otras problemáticas de salud. Es decir, en ese sentido el Ministerio de Salud Pública debería también participar en eso en el sentido de la promoción de la salud. Hay aspectos preventivos respecto a esto que si se podrían trabajar.

14. ¿Existe acceso a la salud mental en el Ecuador?

No. De hecho, la salud mental en el Ecuador es un privilegio. Normalmente lo que observamos es que los servicios de salud como tal son tan pocos y también tan poco rigurosos en el sentido de los mínimos que deben de cumplir para poder dar eso a su población en términos de servicios al público no como consulta privada, porque lo que más existen son servicios de consulta privada, sean los mismos psicólogos que hacemos ese ejercicio de consulta privada o empresas que venden servicios de consulta psicológica. Entonces en realidad en el Ecuador no existen derechos a salud mental. Es simplemente algo que está escrito en el papel, pero en la práctica no se traduce en una realidad en ninguna instancia, ni para quien accede al seguro social ni al sistema público. En el Ecuador sin plata no hay atención psicológica.

**Emilia Piedra**[488]

1. De acuerdo a tu experiencia, ¿qué cambios has observado en el comportamiento en niños, niñas y adolescentes con el aumento del uso de redes sociales en los últimos años?

Bueno, englobando en general a todas las edades, se ha podido demostrar durante las terapias y a su vez en la parte de educación que los niños han cambiado bastante su manera de interacción social sobre todo con sus pares y también entre la familia. Entonces ha llegado a tener un impacto más psicosocial en ellos que entraría dentro del desarrollo cognitivo. Como tu bien sabes, es algo súper fundamental en la infancia de un niño que desarrolle todas estas habilidades tanto en la parte de motricidad, en la parte de lenguaje, también a la vez la parte social, y el hecho de que las redes sociales ahora estén más influyente en ellos hace que se les dificulte en algunos casos el desarrollar todas las habilidades. Si, como te digo, la parte cognitiva está englobada en diferentes aspectos y si uno de ellos no se desarrolla puede afectar a nivel motor, del lenguaje y en diferentes áreas más.

Actualmente ha habido algunos estudios y durante las prácticas realizadas que yo he tenido en mis anteriores trabajos, se ha podido observar un deterioro y un desfase en los niños en relación a su interacción social normal, es decir un niño por lo general empieza a hablar desde muy temprana edad porque tiene bastantes interacciones sociales, el hecho de que no tenga estas interacciones sociales hace que ellos tengan un desfase, es decir, se demoren un poco más en tener este lenguaje que deberían tener en su edad. Sin embargo, en ciertas actividades, no en todas, les va a afectar, si va a hacer muy pronunciado en la parte del lenguaje, interacción social es decir el hecho de no estar conectados con el ambiente y más conectados con una pantalla hace que ellos tengan un problema más que nada con relacionarse; al contacto humano y a su vez al contacto que es externo.

Esto también conlleva a partir de todo lo que fue la pandemia, ha hecho que bastantes niños, bastantes infancias hayan cambiado totalmente. Entonces si bien esto es una herramienta útil para su educación, en muchos casos ha hecho que se haya dado bastante desfase dentro del desarrollo normal de la infancia.

2. ¿Crees que se pueda hablar de alguna adicción al internet y a redes sociales por parte de los niños, niñas y adolescentes?

Si, básicamente, ahora por lo general los cuidadores de los niños suelen tener como una herramienta de distracción o hacer que los niños se sientan más tranquilos si ven algún video. Más que nada por el hecho de que les mantiene toda su atención y su foco en la pantalla. Entonces la verdad si llega a tener un tipo de adicción, no quisiera llamarlo con este término, pero si puede conllevar a que, sobre todo en la infancia en los primeros años de vida, nosotros estamos desarrollando bastantes conexiones neuronales entonces al momento en el que tú estás más de treinta minutos en una pantalla, es decir un niño que tiene tan poquitas interacciones y todas estas conexiones neuronales están enfocadas en esto, va a conllevar a que tenga sobre todo una adicción. Es decir, les va a costar bastante soltarlo, y sobre todo cuando lo mantienes en una rutina, porque los seres humanos en sí somos en base a rutinas, entonces si no tenemos una rutina se nos hace más difícil realizar actividades, estar con nuestro día a día, y lo que un niño necesita en sus primeros años es mantener una rutina en sí. Si tu mantienes una rutina, dándole al niño dos horas diarias el celular, el niño lo va a tener que hacer y si no lo tiene va a conllevar a que efectos

[488] Licenciada en Psicología, ha trabajado con niños y niñas de 2 a 6 años y con la organización Akuankuna para prevenir la violencia en niños, niñas y adolescentes. Entrevistada el 14 de mayo de 2024.

en la parte emocional, efectos en la parte de interacciones sociales, puede que tenga bastantes berrinches, mal humor, y a la vez lo que hace que tengas más de treinta minutos en una pantalla a los primeros años de edad, es decir menos de seis años, hace que las conexiones neuronales que tenemos vayan muriendo. Más que nada, es demasiado fuerte para ellos en los primeros años que tengan toda esta información procesándola en la parte cognitiva.

3. ¿A qué edad sería adecuado, según tu opinión, que el acceso a internet o redes sociales se de en niños y niñas, o no es adecuado?

Creo que, como todas las cosas, si uno puede conllevar un límite creo que, si se lo puede acceder, y también siempre recomiendo que todos los cuidadores de los infantes tengan bastante cuidado con qué contenido están viendo, observando, pero yo creería que tal vez desde unos tres-cuatro años, se podría empezar a utilizar ese tipo de implementos. Sin embargo, no quiere decir que por ejemplo no podemos utilizar canciones. Creo que una de las partes fundamentales que tal vez olvidé mencionar es la parte sensorial, desde que son bebes. Es decir, la parte sensorial conlleva a la parte de audición, de visión, todo ese tipo de cosas que tenemos sensoriales como seres humanos, y podemos utilizarlo como las canciones, videos en algunos casos, para trabajar la parte sensorial. Sin embargo, si es que utilizamos más allá tal vez de unos treinta minutos en un bebe menos de dos años, le va a llegar a afectar un poco. Entonces no consideraría que podemos extender el tiempo sino más bien utilizarlo desde la parte sensorial.

4. ¿Has observado alguna relación entre el tiempo que pasan los niños y niñas en internet y redes sociales, y su bienestar emocional?

En general si, la parte emocional llega a ser afectada porque como te mencionaba que si una de las partes cognitivas está fallando, le llega a afectar a todas indirectamente, entonces por lo general los casos que yo he podido observar a muchos niños les cuesta más interactuar con sus pares, es decir si van a un jardín, si están con su familia, incluso al salir por fuera de la casa, les cuesta bastante interactuar, así sea un saludo o interactuar para jugar con otros niños les cuesta bastante, por lo que conlleva más miedo a enfrentarse a interacciones sociales, lo que va a conllevar a afectaciones emocionales. A su vez, en muchos casos se llega a dar que los niños tienen bastante irritabilidad, entonces el hecho de estar bastante tiempo en una pantalla así sea viendo la televisión o en un videojuego hace que ellos se mantengan más hiperactivos en algunos casos, y en otros casos vayan a tener mal humor, entonces si van a tener repercusiones en la parte emocional. No podría describirte específicamente que parte emocional se ha evidenciado, pero depende del caso del niño.

5. ¿Tú has observado a niños que tienen redes sociales dentro de tu experiencia, o quizás internet?

La verdad sí, creo que desde los dos años tienen bastante acceso al internet ahora. Creo que estamos en una etapa de la vida, en un punto de que es imposible no tener acceso a internet y menos los niños, entonces es un poco normal que todos tengamos siempre el teléfono, la televisión, y veo que siempre les mantiene muy conectados, sin embargo veo que los padres ahora suelen utilizar un poco más esto para poder distraer a los niños, que no hagan tantos berrinches, de estar un poco más relajados en el cuidado de sus pequeños, pero he podido evidenciar que desde muy temprana edad ahora tienen redes sociales. Sus interacciones sociales ahora son por medio de un celular, es decir en casos de adolescentes que he trabajado es normal que un niño de diez años a veces ya tenga celular y se maneje por este medio para hablar con otras personas. Lo que a veces parece que es una herramienta útil, tal vez por emergencia para contactarse con sus padres, es un poco riesgoso que un niño de 10 años que no sepa cómo controlar bien con qué personas interactúa mantenga una red social, porque pueda que, si se contacte con sus amigos,

pero también pueda tener acceso a otras cosas. Justamente ahora hay varias estafas, robos y muchas personas que pueden ser mal intencionadas y utilizan justamente las redes sociales para poder conocer a personas que son minorías o personas que realmente no tienen todo el conocimiento en sí para tener el cuidado debido de tener un teléfono o una red social como son los niños y adolescentes. Entonces, si tiene su ventaja en algunos casos, por ejemplo, puede ser una ventaja poder aprender canciones o estudiar en sí, pero creo que la mejor manera de poder aprender para los niños o adolescentes en educación no es siempre la tecnología. Por mi parte como psicóloga yo no lo recomendaría como un método 100% de estudios sino más bien como una herramienta a la educación que tenemos.

6. ¿Qué impacto crees que tienen las estrategias de diseño de las redes sociales, como las notificaciones constantes, etc., sobre la salud mental de los niños, niñas y adolescentes?

Bueno, creo que dependería del tiempo en el que tú tienes acceso a este tipo de herramientas, tal vez como el celular que nos presenta bastantes notificaciones, pero en algunos casos sobre todo en caso de niños que tienen TDH o niños que cuentan con algún tipo de ansiedad que bueno ya vienen a ser más niños, niñas y adolescentes o adolescentes, les puede generar más ansiedad ante las situaciones que ya están atravesando cotidianamente, es decir por ejemplo en algún caso que yo vi en el trabajo: había una adolescente de que el hecho de que simplemente que le lleguen notificaciones por alguna x razón, le generaba más ansiedad de lo que generalmente ella ya presentaba, entonces dependería bastante del caso, sin embargo yo considero que les hace estar un poco más en alerta y tener un poco más de apego a estas plataformas. Entonces creo que sobre todo las notificaciones son algo que a veces tal vez nos puede ayudar a nosotros para recordatorios y ese tipo de cosas, pero a veces nos puede volver un poco más con este apego de estar constantemente revisando el celular o el aparato que tengamos.

7. ¿Cómo se maneja esto de la ansiedad, esta línea que me comentas, cómo te dabas cuenta?

Bueno, esta adolescente ya tenía diagnosticado un poco de ansiedad, no tenía todos los rasgos, pero si presentaba bastante ansiedad sobre todo porque su contacto e interacciones sociales siempre eran con el celular, entonces su manera de relacionarse en el colegio casi no era, y las personas con las que interactuaba eran virtuales, es decir sus amigos eran de otros lugares, se contactaban a través del celular, y el hecho de que a veces ella sienta esta ansiedad de que no está respondiendo a tiempo, de que debería estar ahí, a veces le generaba angustia y sobre todo malestar el hecho de estar constantemente teniendo que estar pendiente más en el celular, más en el mundo virtual que ella tenía porque sus interacciones sociales las tenía ahí, más que estar en el "aquí", en el presente, en la parte real. Entonces si le generaba un poco de ansiedad el hecho de estar olvidando no responder porque aparte para ella esto era muy importante. Como te digo es dependiendo del caso, pero en este específico, a esta persona le generaba mucha angustia el hecho de olvidar este mundo virtual que ella tenía aparte porque en el caso de ella no tenía interacciones, no tenía amigos en el colegio, más se dedicaba estar en videojuegos, justamente estos amigos los tenía por los videojuegos. Era como tener una segunda vida; estar aquí y en la pantalla.

8. ¿Has notado diferencias en como los niños, niñas y adolescentes reaccionan emocionalmente a las interacciones en línea en comparación con las interacciones personales, físicas?

Si, como te digo, ahora desde muy temprana edad suelen tener bastante atención centrada en la pantalla, en los juegos y les llega a causar mucho conflicto en el momento que quieren relacionarse en persona. Por ejemplo, los niños de ahora, he visto bastante, que tienen apego

ansioso. Es algo normal que en las infancias se lleguen a dar diferentes tipos de apego, pero uno de ellos que se ha presenciado más es el apego ansioso ante la familia, ante situaciones donde usualmente suelen estar porque el hecho de estar bastante tiempo en la pantalla hace que no tengan la necesidad de que tengan que salir a interactuar con otras personas, es decir tener una interacción más entre sus pares, entre sus mismas edades, en la escuelita, en el jardín. En muchos casos les llega a dar apego ansioso con la mamá, es decir yo he tenido bastantes casos desde empecé a trabajar de niños que se les llama "niños pandemia" porque nacieron justo en la pandemia o fueron bebes cuando pasó todo esto, entonces lo que sucedió fue que no tuvieron interacciones cercanas, o acceso a interacciones regulares como el caso de todos nosotros que fuimos a un jardín de niños, y con estos niños se evidencia realmente que ni siquiera pueden decir "hola", les cuesta demasiado el siquiera tener una interacción en contacto visual, y no me refiero a niños que tengan algún tipo de trastorno o discapacidad en sí, sino niños en general. Les cuesta demasiado tener esta interacción social entre ellos y con sus pares.

9. Este negocio de las redes sociales, del internet, que toman datos de las personas, las mercantilizan y las utilizan para saber que les gusta, y de esta manera que estén más tiempo en pantalla: ¿cómo se podría contrarrestar?, ¿tú consideras que este modelo de negocio está directamente relacionado con estos problemas de salud mental en niños, niñas y adolescentes?

Creo que actualmente están intentando enfocarse un poco más en la salud mental en las últimas décadas, entonces hay diferentes plataformas que, como te digo, ayudan mucho para la educación de los niños, tratan de buscar herramientas, más que hacerles un daño ayudan a que las infancias sean más tolerables, más divertidas.

Creo que, en sí, cómo se podría contrarrestar conlleva más entre los cuidadores, porque las plataformas muchas veces, por ejemplo, si tu entras a cualquier plataforma que son para ver películas, videos, donde tú quieras, puedes siempre poner la categoría de niños, siempre puedes poner actividades que sean de acuerdo a la edad. Sin embargo, las personas responsables en sí del tiempo, la calidad y el contenido que consumas los infantes siempre va a ser de los cuidadores porque son ellos los que tienen el control en sí de las herramientas.

Entonces mi consejo sería que los cuidadores se tomen más en serio a qué contenido están dando acceso a sus niños y a la vez dando algunas limitaciones, que es lo que muchas veces y actualmente veo que es lo que les cuesta bastante poner límites en los niños no solamente con las aplicaciones sino con otro tipo de actividades. Así que sería con los cuidadores y a su vez las plataformas también deberían tener más control entre qué contenidos hay y a su vez el tiempo en el que se pueda trabajar, por ejemplo, hay herramientas ahora de juego en donde puedes poner el tiempo de utilización de esa aplicación.

10. ¿Qué recomendación podrías dar a las empresas para prevenir estos impactos que ya se están dando en los niños, niñas y adolescentes con el uso de estas plataformas?

Las empresas deberían poner más controles, como, por ejemplo, límites de tiempo a los niños, niñas y adolescentes. Asimismo, deberían educar a las personas consumidoras de sus servicios sobre los impactos en la salud mental que podrían generar su consumo. He observado de cerca las dinámicas de uso de dispositivos digitales en niños pequeños. Éstos están expuestos a contenido que puede ser dañino para su salud mental. Además, genera comparaciones, y las notificaciones pueden generar ansiedad. Todas estas cosas deberían ser debidamente informadas, tanto a los cuidadores como a los niños y niñas.

**Fernando Ocaña**[489]

1. ¿Qué cambios has observado, desde tu experiencia, en el comportamiento de niños y niñas con el aumento del uso de internet y redes sociales en los últimos años?

Bueno, puedo decir que tengo un poco más de experiencia con adolescentes, pero de igual manera he podido constatar que las relaciones de este grupo poblacional se están basando ahora exclusivamente a aspectos digitales, principalmente de las redes sociales. No es raro ya ver a niños, niñas desde los 10 años más o menos, que ya tienen redes sociales, que chatean con sus compañeros, que están en ciertos grupos, y claro, se basa mucho ahora su interrelación con estos medios digitales. Claro que no podemos decir que sea algo completamente negativo porque estamos en la era digital, y hay que aceptar que mientras la tecnología sigue avanzando, pues las nuevas generaciones principalmente deben ir adaptándose a estos cambios digitales, cambios virtuales. La ciencia nos dice que está avanzando a pasos agigantados. En apenas 30 años se evidencia el gran cambio tecnológico y de aquí a los que vienen, se augura tener cambios incluso más grandes. Así que niños, niñas y adolescentes no están ajenos a esto. Recordando que ellos están aprendiendo, y bueno justamente la etapa de niños y niñas están aprendiendo del reflejo y quien es su reflejo, bueno su familia: de lo que ven de sus padres, de sus madres, de sus familias, con quienes convivan, lo que ven de sus hermanos; si tienen hermanos un poco más grandes, este aprendizaje por reflejo es natural, pues se va profundizando un poco más en estas generaciones que ahora tienen una facilidad de acceso tan grande a los recursos tecnológicos. Así que, en ese sentido es algo natural y que se espera. Ahora, las consecuencias que trae no manejarlo, es otra cosa.

2. ¿El acceso a la tecnología, podría convertirse en otra brecha más en diferenciar más a las clases sociales? ¿Cómo observas este fenómeno del acceso respecto a las redes sociales, internet?

Yo puedo ver que más bien esa brecha se está comenzando a reducir. He trabajado con niveles socioeconómicos muy diversos y he podido constatar que, aunque socioeconómicamente se encuentren en situaciones bastante complicadas, hay un recurso tecnológico que generalmente no falta y se está volviendo algo simbiótico de los seres humanos, de las personas. La mayoría de celulares son de tipo inteligente, y el acceso a estos recursos pues es mucho más visible, claro que no puedo dejar de lado que si pueden existir un grupo de personas que aún no pueden acceder porque si están en una situación de precariedad económica, pero por otro lado pues si es evidente, y es un objeto primordial, ahora se siente y más bien, se hace notar como algo completamente necesario el uso del celular. En ese sentido partimos desde una catástrofe mundial, que fue lo del COVID, lo del encierro, y que eso obligó a que todas las familias de alguna u otra manera busquen esta herramienta tecnológica porque la educación se lanzó al ámbito virtual. Tengo que hablar que se "lanzó" porque nadie estábamos preparados para la virtualidad, nadie. Ni los docentes, ni los mismos estudiantes, entonces se vieron obligados a buscar formas de obtener este recurso: sea por donaciones, por préstamos o sea que se endeudaron algunas personas porque necesitaban acceder, porque sus hijos prácticamente muchos aprendían desde el celular. Y también eso marcó la necesidad del internet, porque claro, no servía de nada tener el celular si no tenían internet.

---

[489] Psicólogo Clínico, especialista en educación y nuevas tecnologías de comunicación e información por la Universidad Andina Simón Bolívar. Analista del Departamento de Consejería Estudiantil de la Unidad Educativa Aviación Civil. Entrevistado el 21 de mayo de 2024.

Entonces, si he podido evidenciar que esas consecuencias que arrancan bajo la pandemia nos arrojó también mucho más al mundo digital. Ahora podemos utilizar estos recursos de video llamadas, algo que antes de la pandemia era muy poco usado. Yo puedo decir que era muy poco usado, solo en aspectos puntuales y ahora es algo natural, todo el mundo sabe qué es el zoom, ya está en la jerga poblacional, uno escucha "zoom" y ya sabe que es video conferencia. Entonces yo puedo decir que esa brecha si se ha ido reduciendo, no está completamente reducida, aún existen poblaciones que no tienen acceso completamente libre a estos recursos tecnológicos, pero siento que poco a poco se va reduciendo un poco más. Además, que estos recursos tecnológicos están bajando su acceso económico, ahora por lo bajo una persona puede obtener un celular barato y que puedan conectarse a internet en unos 50-80 dólares. Ahora es mucho más sencillo ver a los niños y a las niñas, principalmente a los adolescentes con celulares, es bien raro verlos sin celulares, muy raro.

3. ¿Qué tipos de problemas de salud mental ha visto asociados con el uso de internet y redes sociales en niños, niñas y adolescentes?

Bueno, ahí si es un tema bastante largo. En varias investigaciones que se han enfocado en salud mental, también a raíz de la pandemia y el encierro que tuvimos, puedo destacar algunos principales: el primero es el punto de la relación; este desafío de relacionar porque es un desafío pararme frente a una persona y relacionarme con ella, eso se está evidenciando un poco más con las generaciones que están más inmersas en el tema digital, que ahora la relación se basa básicamente en una pantalla, la interrelación que tienen ellos de forma directa se está reduciendo mucho y esto está causando varios problemas enfocados en el aspecto de violencia. Yo como miembro estudiantil de docente tengo una misión principal que es abordar el tema de la violencia y la violencia digital se ha incrementado de manera increíble. Puedo poner un antes y un después de la Pandemia, si había violencia digital, pero después de la pandemia donde nos hemos arrojado todos un poco más a la virtualidad, se ha incrementado exponencialmente. Es un incremento generacional e increíble de la violencia.

¿Por qué se da esto? Porque los medios digitales, principalmente las redes sociales, no tienen filtros de control para todo lo que se comparte. Hablemos de WhatsApp, Instagram, Facebook, Linkedin, hablando de todas las que hay, no hay un control real sobre qué se comparte. Y es un punto de lo que mencionabas al inicio, que estás redes están enfocadas en tener el mayor número de información que puedan obtener de nosotros, y es lógico que no ponen restricciones para poder prevenir situaciones de violencia. El anonimato que da las redes sociales propicia que este grupo que no maneja aún sus emociones: niños, niñas y adolescentes, no saben cómo gestionar sus emociones son aún ególatras y es algo natural, solo piensan en sí mismos y en sus deseos, no piensan en lo que pueda suceder, no piensan en las consecuencias, ese anonimato les da la carta abierta para violencia, insultos, mensajes ofensivos, chismes, imágenes grotescas. No tienes una idea de la cantidad de violencia que ahora se está manifestando en las redes desde los niños donde se insultan, crean páginas. Desde pandemia y un poco más hay un boom de los "Confiésate" no sé si tal vez has escuchado de esto. Es una página que se crea en una red social sea Facebook o sea Instagram, sea cual sea, se ponen "Confiésate" y el nombre a la institución que pertenecen, como, por ejemplo: "Confiésate COTAC".

"Confiésate" es una Fan Page que crean los estudiantes anónimos porque nunca ponen su identificación para que sus compañeros compartan chismes, declaraciones, imágenes, memes ofensivos, es decir, que compartan todo lo que les da la gana. Y hay una premisa principal en todos los "Confiésate", es una palabra que los niños, niñas y adolescentes utilizan: en cada post que hacen en los "Confiésate" al final ponen "TAPA". Yo no entendía desde mi diferencia generacional, lo asemejaba al "tapa" de "tonto", y el "TAPA" ha sido el "no digas quien soy",

porque ellos a la Fan Page mandan mensajes para que publiquen el mensaje, pero les ponen que no divulguen quien es. El que maneja la página nunca se muestra porque sabe sobre las graves consecuencias que tendrá, porque está promoviendo violencia, peleas. Donde publican peleas, chimes, que promueve a que en el recreo se agarren a la entrada y salida, se insulten, amenacen, se agreden. Por los "Confiésate" ha habido situaciones bastante graves, incluso en donde ha habido intentos de suicidio por el acoso tan grande las víctimas.

Ahora que los niños, niñas y adolescentes están metidos mucho más al ámbito digital, son mucho más propensos a el daño emocional que crea lo que ahora se llama el "HATE". Esto causa graves secuelas emocionales. Si he tenido situaciones de intentos de suicidios por la carga emocional que implica esto. Para nosotros como institución es muy difícil identificar quiénes fueron porque no tenemos los recursos tecnológicos o no tenemos la forma de saber quién fue. Se hacen las denuncias en fiscalía, incluso ya hay una fiscalía de delitos digitales, pero soy completamente sincero porque no se llega realmente a una resolución. Lo único que hacen es cerrar la página. Entonces cancelan la página, pero vuelven a crear porque es algo sumamente sencillo. Generalmente hacemos campañas entre padres y docentes para que cierren las páginas y denunciar. El algoritmo de esta página entiende que, si hay una gran cantidad de personas denunciando, ahí si consideran que es malo y lo cierran. Cierran la página, pero esta persona que está en el anonimato vuelve a crear una. Este es el problema que más siente en boga desde instituciones, escuelas y colegios.

La situación de problemas de autoestima también ha crecido bastantísimo porque es mucho más sencillo proyectar una imagen digital, porque ahora tenemos filtros: filtros que cambian, que ocultan ciertas características, ciertos aspectos que puede que no me agraden de mi físico, y priorizo mostrarme desde ahí, pero de forma presencial es decir cara a cara no lo hago. Esto también se arrastró con la pandemia, los niños, niñas y adolescentes ahora priorizan el uso de la mascarilla, pero no es por situaciones de salud, es por situación de problemas de autoestima, en donde no quieren desprenderse de la mascarilla porque no quieren que vean su rostro cien porcientos, piensan que su rostro no es atractivo o puede ser motivo de burlas y demás, pero en cambio en redes sociales si se muestran con todos los filtros que puedan utilizar. Hacen videos, hacen tik toks y todo lo demás, pero ya con las personas de frente es mucho más complicado.

Y pues los problemas comunes que se dan en el ámbito digital son las extorciones, el sexting, situaciones relacionadas a estos aspectos relacionadas a la violencia digital aún se siguen presentando y se seguirán presentando porque las personas normalmente no saben relacionarse de otra forma que no sea con violencia. Esos son los graves efectos que en este momento se están presentando y que se reflejan en términos emocionales. Los niños, niñas y adolescentes ahora son más propensos a dejarse dominar por su ansiedad, frustración, tienen una actitud inmediatista donde no hay paciencia. Los medios digitales también nos están habituando a que las cosas sean inmediatas. Whatsapp por ejemplo puso eso que sirve para acelerar las notas de voz, le pones al 2x para escuchar rápido, pero en realidad no escuchas bien. Tik tok empezó con segundos y pasa, y eso psicológicamente es algo que los niños, niñas y adolescentes están habituándose, y mucho más los niños y niñas. Si tú pones a un niño que se habitúe a estar con su cerebro activo porque a cada rato está viendo algo diferente, pues va a crecer como una persona que está buscando aspectos inmediatos, satisfacción inmediata y esto a largo plazo se va a ver en el aumento de trastornos de ansiedad, estrés, bajo nivel de la frustración, todo eso se va a ir evidenciando, claro que no de forma inmediata porque estamos hablando de que varias generaciones en donde tendríamos que ver la presencia de estos trastornos psicológicos y psiquiátricos que se van presentando a lo largo del tiempo pero que claro tienen también características e influencia sobre cómo se han ido manejando en estos entornos digitales. Ahí radica si se tienen que tomar acciones pronto porque puede ir complicándose un poco más.

4. ¿El internet ha potenciado los niveles de violencia en las relaciones de niños, niñas y adolescentes? Quisiera entender es que si ¿tú ves el acceso al internet como algo negativo?

No, por supuesto que no. El internet, la Tablet, la computadora y todos los recursos digitales son una herramienta, ninguna herramienta es mala ni buena. El uso que le damos es el valor que tiene. Por ejemplo: un cuchillo sirve para cortar el pan, como una herramienta de trabajo, pero también puedes matar con un cuchillo. El internet y todas las herramientas digitales son eso, nos ayuda a nosotros a realizar varias, muchísimas actividades. No podemos negar que el avance tecnológico y el que va a venir va a ser extraordinario. 30 años de diferencia y te puedo decir un poco más, 60 años. Si vemos de 60 años acá y trajéramos a una persona de esa época, pensaría que todo esto es de película. Básicamente mucho de lo que se planteaba en la ciencia ficción actualmente lo tenemos. Tenemos realidad virtual, interacciones virtuales, tenemos tantas cosas y lo que viene. La ciencia nos dice que todo lo que es tecnología, cada año es como si pasaran cinco años. Avanza de manera incontrolable. Ya hay inteligencia artificial. Nosotros nos creíamos los únicos seres inteligentes del universo en gran medida, y ahora hay algo que también tiene inteligencia, que no está vivo y que es una creación nuestra. Vamos a convivir con robots. La tecnología nos va a dominar por completo así que tenemos que saber cómo utilizarla de manera beneficiosa, no solo para mí, sino también para la sociedad, y eso es lo que tenemos que enseñar a las nuevas generaciones. Que esta herramienta tiene sus riesgos y sus grandes peligros.

Las generaciones que están más arriba que las nuestras son analfabetas digitales. No saben cómo realmente se maneja y se tiene que trabajar, y como no lo saben utilizar no nos enseñaron cómo utilizarla de la mejor manera y los que no han aprendido a manejarla de la mejor manera, van a enseñarles a sus hijos e hijas lo mismo; lo que saben, lo que no saben, y se va a seguir repitiendo el círculo en donde una herramienta tan poderosa y tan importante se las deja en manos sin ningún cuidado o control.

5. ¿Cree que exista una relación entre el modelo de negocio, internet, redes sociales y el aumento en problemas de salud mental de niños, niñas y adolescentes?

Exactamente, es un negocio y que radica en que lo que grandes filósofos de la historia nos han dicho: La información es poder, el conocimiento es poder. El internet es el arma más peligrosa y más poderosa del mundo entero, la estamos utilizando en este momento y no somos conscientes de ese gran poder porque no quieren que seamos conscientes de eso, porque al no ser conscientes somos mucho más manipulables y al ser manipulables somos consumidores, ciegos frente al producto que nos venden. Los niños y niñas por supuesto que están siendo absorbidos por este giro de negocio en donde ya no es necesario un intermediario que era un poco más controlado, como la televisión, los medios impresos, tenían filtros y controles, ahora ya no es necesario. Ahora te puedes hacer pasar por un adolescente y venderles drogas, que son cosas que pasan.

Cuando yo inicié la pandemia, puedo decir una anécdota muy personal, ahí me di cuenta de lo peligroso el aparto que tenía. Recuerdo que mi sobrina me pidió que le compre unas "Bratzs", y me preguntaba ¿dónde me voy a conseguir esas muñecas? Y decía el nombre de la muñeca porque no sabía dónde voy a comprar y como estaba trabajando en el celular, en el computador después en mis redes sociales comenzó a aparecer la publicidad de esas muñecas. Yo me sentí en ese momento asustado, más que asustado horrorizado. Eso es violentar nuestra privacidad porque nos están escuchando y también están escuchando los niños, niñas y adolescentes y por supuesto que a ellos también les van a aparecer las publicidades de los productos un poco más personalizados. Ahora hablamos de publicidad directa. Todo esto llega al

inconsciente. El celular va a todas partes con nosotros, hasta al baño, es simbiótico. Ahora es mucho más fácil para las empresas que nos ofrezcan sus productos de forma personalizada, pues a nuestros niños, niñas y adolescentes serán más influenciables.

6. ¿Qué recomendaciones darías a los padres, los cuidadores en general, para abordar los riesgos de la salud mental asociados con el uso de internet en niños, niñas y adolescentes?

Lo primero sería educarse. No podemos combatir los problemas que crea el mal uso de las herramientas digitales si no estamos completamente preparados y conocemos: qué es y cómo se utiliza, porque la idea es enseñarles a utilizar de manera correcta, pero como te mencionaba, lamentablemente hay una gran cantidad de personas de generaciones arriba que son analfabetas digitales. Tengo docentes que se prepararon para educar y son analfabetas digitales. Siendo nativos digitales, podríamos ir activando los controles. Hablando de niños, niñas y adolescentes lo primordial es los tiempos. Lo ideal y lo que nos dice la ciencia es que niños y niñas niños, niñas y adolescentes de cinco años no deberían estar frente a las pantallas. Sabemos que en la realidad es muy difícil. Mientras van creciendo la idea es ir aumentando poco a poco el tiempo que tienen a la exposición de las pantallas porque primero tienen que conocer y saber utilizarlas.

Priorizar de igual manera la interacción social, en el que las relaciones sociales sean un complemento, pero no suplanten la relación social directa, y ¿cómo hacemos eso?, pues con el ejemplo. Desde las familias vamos formando a nuestros hijos e hijas que se vayan interrelacionando. Esa es una idea primordial del uso correcto del tiempo y de esa manera también estamos reduciendo mucho el uso de pantallas y estamos priorizando la interrelación.

Las protecciones de riesgos digitales también son importantes. Las redes sociales, todas, tienen control parental, el celular tiene control parental, las computadoras también, todo actualmente tiene control parental. Por eso tengo que ser un nativo digital porque tengo que utilizar los recursos. Si yo le voy a dar una computadora a mi hijo va a utilizar el buscador, tengo que crearle una cuenta y tiene que ser una con control parental, quiere decir que va a tener enlace directo con mis cuentas. Yo le creo la cuenta de correo electrónico y esa cuenta la enlazo con la mía y de esta manera estoy controlando qué tipo de material o productos está consumiendo. Muy pocas personas activan control parental. Los muchachos que son mucho más hábiles por la diferenciación generacional desde el ámbito tecnológico saben más que los mismos padres. El conocimiento de la tecnología ahora es de las nuevas generaciones. Incluso hay que saber las trampas que existen para poder pasarse los controles parentales. Hay niños, niñas y adolescentes que incluso ya no priorizan el uso común, sino que priorizan irse por lo más peligroso que se conoce como la “DEEP WEB”.

Si tú hablas con adolescentes de estas generaciones, de diez, yo te puedo decir que cuatro ya han entrado a la Deep Web o que saben entrar a la Deep web y que ya han estado por ahí curioseando lo que hay ahí. Hay algunos que incluso avisan que han ido hasta lo más profundo de la Deep Web y eso está aumentando. En otros navegadores que podría decir que son “más seguros” también pueden tener material muy destructivo para su salud mental, en la Deep Web encuentran verdaderamente horrores y acceso a material completamente perturbador. Todo esto ataca principalmente a su salud mental y se puede ver reflejado en aspectos ya mucho más físicos dependiendo del material que consuman.

7. ¿Qué papel cree que deberían desempeñar las empresas de redes sociales para mitigar los impactos negativos sobre la salud mental de los niños, niñas y adolescentes?

Desde lo que son las empresas de redes sociales principalmente, sería tener un compromiso mucho más fuerte con la salud mental. Estas empresas están enfocadas

principalmente al lucro entonces la salud mental siento que verdaderamente no es algo que está dentro de sus prioridades más bien es algo que en cierta medida lo sienten obligados. Yo te puedo decir que soy un consumidor de tik toks y llega un mensaje a veces en el que dice "oye te has quedado mucho tiempo aquí, mejor sal, disfruta, sal con tus amigos", es un mensaje recordatorio de que estas muy metido en ese mundo y de que salgas. Yo creo que eso pasa cuando sobrepasas los cien videos. Creo que si podemos dar ese recordatorio con una cantidad menor, para decir "estás consumiendo mucho esto, mejor haz otra actividad". El tener estos filtros para poder ir combatiendo esos aspectos como la violencia también es algo importante. Hay mucho material en las redes sociales que están cargados de violencia. Incluso ahora la violencia está mucho más implícita y es básicamente porque se pone a criterio del que hace el video saber qué produce y qué comparte. Es violencia, yo siento, muchas imágenes que se publican o videos que tratan de saltarse las seguridades. Hay estos famosos "TRENDS" que son videos virales que se hacen con una temática. Hubo un trend en el que se sexualizaba mucho a los hombres en donde ponían imágenes indirectas en el que se podía ver sus penes. Y pienso en que esto se puede encontrar mi sobrina, un muchacho o una muchacha. El algoritmo no lo detecta como violencia, lo detecta como un material cualquiera, pero está ahí. Porque claro, el material educativo no se hace viral, el material que enseña no se hace viral. Estamos en un punto de la sociedad en el que lo que es viral es el amarillismo, y el amarillismo es violencia, es todo lo relacionado al sexo, todo lo relacionado a la sexualidad a las drogas y eso es lo que más consume la gente. Hay una estadística sobre cuántos "likes" recibe este contenido y el contenido educativo y es abismal.

Desde lo educativo es importante enseñar a utilizar esta herramienta. En el Ecuador lamentablemente desde el 2015 se eliminó la materia de computación, en donde si quiera en las escuelas y colegios mal o bien, nos enseñaban a utilizar este recurso. Se eliminó. Porque los políticos de ese momento pensaban que ahora todo el mundo tiene la computadora en la casa, tienen celulares entonces ya no necesitan aprender a utilizar. Sabemos que los ecuatorianos no somos autodidactas, eso puede funcionar en una cultura completamente diferente, pero en nuestra cultura no, en nuestra cultura yo no busco aprender lamentablemente, me tienen que enseñar obligado. Somos una cultura que está acostumbrado al "Big Brother": alguien que esté arriba enseñándome o que me obligue a que haga algo. Es cultural. Eliminar esta situación cultural es muy difícil. Al eliminar la cátedra de computación desde el ámbito fiscal, haciendo una diferenciación de clases, el recurso que se podría utilizar de manera óptima para que los niños, niñas y adolescentes puedan utilizar bien esto ya no existe y está creando una gran brecha generacional y socioeconómica porque si tú le pones a un joven de un colegio particular a utilizar una computadora la va a usar bien, pero en cambio le pones a joven de un colegio fiscal te va a patalear.

En una ocasión, con un grupo de tercero de bachillerato que están a punto de salir al ámbito profesional yo apliqué un test vocacional en los laboratorios, les puse el link, y les solicité que por favor guarden la información porque era un tipo Excel, y decían "¿y cómo guardo?", y yo les respondía "denle click al disquete", y ellos decían "¿qué es disquete?", y yo me quedé anonadado. Tuve que enseñarles qué es un "disquete" a pesar de que estaba frente a ellos, y no sabían hacerlo. Pero en redes sociales si saben todo. Entonces la educación es una clave primordial y de esta manera disminuirán los riesgos y empezaríamos a utilizar todo de una forma óptima esta gran herramienta que es la tecnología.

8. ¿Crees que existe acceso a la salud mental del país? ¿qué podrían hacer las organizaciones de la sociedad civil para mitigar estos daños?

Acceso a salud mental muy poco. No puedo decir que no existe, pero muy poco. Tenemos una ley de salud mental que fue aprobada en enero y hasta ahora no es aplicable entonces podemos

tener en el papel, pero en la realidad no hay. Cuando derivo a mis estudiantes al necesitar atención psicológica se encuentran con la novedad de que no hay citas porque hay un psicólogo, uno solo, por cada centro de salud, por hospital puede que haya dos, y tienen que tratar a muchas personas.

Creo que el punto de la lucha social es algo importantísimo. Sin lucha social verdaderamente no podemos proponer cambios significativos en una realidad completamente caótica, principalmente por los aspectos políticos y el mal funcionamiento de los gobernantes. Creo que la organización civil tiene que reorganizarse para verdaderamente exigir que la realidad comience a cambiar. Si también hay la posibilidad de que se provean de recursos, porque ahora lo que nos falta son recursos. Si yo necesito salud mental, requiero de psicólogos y si hay psicólogos que están sin trabajo y son muy necesarios, exijo. Recientemente hicieron un análisis en el que reducir el bolsillo del estado es botar maestros, médicos, psicólogos y policías porque donde hay mayor gasto del estado es ahí. Si queremos servicios necesitamos recursos humanos. Los gobiernos anteriores se olvidaron del recurso humano. Los psicólogos del colegio estamos completamente saturados. La ley reformatoria de la educación del año 2019 te dice que los profesionales de los departamentos de consejería estudiantil debemos tener como máximo 450 estudiantes a nuestro cargo, recordando que ese número se triplica porque trabajamos con las familias. Pero actualmente los DS tenemos 800, 900 o 1000 estudiantes a cargo. Conozco un compañero en provincia que tiene 2000 estudiantes a su cargo. Entonces yo me pregunto ¿cómo podemos promover salud mental si tenemos 2000 estudiantes a nuestro cargo? Personalmente yo tengo 900 estudiantes a mi cargo y no me abastezco, no puedo llegar con prevención, no puedo ni siquiera hacer las entrevistas porque los casos aparecen y siguen, y siguen, y es completamente desbordante. Creo que la comunidad civil debe reorganizarse, porque sin lucha social verdaderamente no podremos promover un cambio.

**Henry Zaruma**[490]

1. ¿Qué cambios has observado en el comportamiento de niños, niñas y adolescentes con el aumento del uso de internet y las redes sociales en los últimos años?

Creo que lo que más se puede notar evidentemente es un uso más habitual del internet, las redes sociales, tecnología, tablets, teléfonos, cualquier dispositivo que existe pues ahora es mucho más habitual que hace diez años por ejemplo, obviamente el tema del acceso a la tecnología, al internet se ha venido incrementando y eso hace que prácticamente niños desde muy pequeños tengan a su disposición un celular, una Tablet o cualquier dispositivo que se convierta prácticamente en algo cotidiano o algo necesario y no solamente eso, sino también el internet, las laptos, televisiones. Llegaría a pensar que es muy complicado llegar a tener una vida apegada más o menos con todas estas comodidades sin todo eso. Es parte de nuestra vida, pero ahí hago un pequeño análisis: obviamente si vivimos en el sector urbano, esto es lo habitual en el sector urbano, en el cotidiano, pero no es la misma manera para las familias, adolescentes, niños, niñas y adolescentes quizás en el sector rural. Entonces eso también hay que considerar de acuerdo a la manera en la que se accede a este tipo de información. Incluso teniendo en cuenta el tema de la clase social. Es posible que en un domicilio solo haya personas de clase media, un poco empobrecidas y que solamente haya una computadora en la casa y eso evidentemente va cambiando a diferencia del joven, del adolescente que tiene un celular, una Tablet, una televisión en su cuarto y aparte de eso tiene internet. El acceso a la información es parte de los derechos que también tenemos las personas y de qué manera lo están viviendo teniendo en cuenta esta variable de clase social. Y cómo lo viven los adolescentes de comunidades de la Amazonía donde quizás no hay una conexión a internet y a que información pueden ellos acceder, es decir que no está democratizado, es más complejo.

2. ¿Qué tipos de problemas o impactos has visto asociados con el uso del internet y redes sociales en niños, niñas y adolescentes? ¿crees que el internet es bueno o malo?

Por ejemplo, algo que se nota con los niños, luego de la pandemia, casi dos años que los niños estuvieron en casa con sus padres y sus padres trabajando, en el mejor de los casos teletrabajando, y esos niños eran niños de tres o cuatro años. Pensemos en que ellos, quizás cuando inició la pandemia tenían un año o algunos meses nada más, pero nunca habían estado en un ambiente escolar, y a lo largo de todo ese tiempo, la única interacción que tuvieron fue la que podían tener en casa con sus padres. Un efecto que se observa en ese sentido con los niños pequeños, fue la mayor incidencia en problemas del lenguaje porque cuando está en interacción con las personas a través del lenguaje esa comunicación nos va influyendo, entonces recordemos que en la comunicación hay lenguaje verbal, no verbal la relación. Es lo que dice Paul Watzlawick en Los Axiomas de la Comunicación Humana.

A través de la pantalla no se pueden ver este tipo de situaciones como por ejemplo el tono de voz con el que te digo las cosas, mi expresión, como se mueven las manos, pero por ejemplo estos niños empezaron a tener y se observaba una mayor incidencia en problemas del lenguaje porque les sentaban frente al computador y a través de la televisión o cualquier otro dispositivo, les ponían música, y el niño estaba pasivamente recibiendo las estimulaciones, videos, etc. Pero cuando todo eso tiene que volverse productivo a través del habla, ahí es cuando nosotros los

[490] Psicólogo en el Departamento de Consejería Estudiantil de la Unidad Educativa Bilingüe Julio Verne, estudiante de la maestría en adolescencia y Juventud de la Universidad Andina Simón Bolívar, sede Ecuador. Entrevistado el 28 de mayo de 2024

psicólogos, los psicopedagogos veíamos que los niños empezaban a tener muchos problemas del lenguaje y se notó con mucha preponderancia luego de volver de la pandemia.

Vamos con niños un poco más grandes como de ocho a diez años. Sucedió que estos niños, como pasaban la mayor parte de su tiempo utilizando un computador, celular, tuvieron acceso a un montón de información y parte de esta información fue de contenido pornográfico. Entonces nosotros cuando regresábamos a los colegios se veía que sus comportamientos estaban muy sexualizados, en situaciones de juegos, que podían verse desde la mirada del adulto no apropiadas a su edad, pero estaban exacerbadas estas conductas porque cuando se notaba, y no solamente en videos contenidos explícitos sino hasta en la música, porque venían con el reggaetón y esto es algo que ha influido. Si vamos en esa misma línea con los adolescentes, por ejemplo, tenían muchos sentimientos de ansiedad, de depresión que les fue afectando a su salud mental. No poder socializar, cuando en la adolescencia es fundamental, es algo que les afectó.

Antes te mencionaba esta variable de la clase social, pero, ¿qué pasa con el género en adolescentes? Las mujeres adolescentes y niños, niñas y adolescentes viven más procesos de vulneración a través de redes sociales porque hay una imagen que se proyecta a través de estas redes y es la imagen de una mujer esbelta, todo lo que implican estos estereotipos. Esto se refleja en trastornos de la conducta alimentaria, trastornos en problemas de la imagen, si tomamos en cuenta esta variable de género también. Entonces las cosas más habituales que suceden con los adolescentes en particular es esto de estarse constantemente comparando quizás con otras personas, con otros cuerpos. Su propia vida se compara en cuanto a lo que se ve a través de esta ficción y que a la final es lo que se vende. Y ahí está lo que tú me explicabas un poco, de como es este tema de la matriz productiva que sustenta todo esto, y el tema de los datos de los adolescentes que es fácilmente explotable de alguna manera porque nos ponen en una matriz en donde el consumo y el hiperconsumismo de los cuerpos, de la mercancía, de la naturaleza. Estamos constantemente en ese dinámica, entonces cuando los chicos ven un video en tik tok o en cualquier red social, aparece este fenómeno de la comparación: “Yo no tengo este cuerpo”, “Yo no tengo esta casa”, “Yo no tengo estas cosas”, y los chicos entran en esta lógica de consumir y seguir reproduciendo esta matriz productiva y con eso creo que el sistema económico que está sustentando esto se ve beneficiado porque están justamente valiéndose de todo esto para poder obtener lo que ellos quieran pero a qué costo, a todo este costo que como psicólogos observamos con los chicos.

3. ¿Qué impacto crees que tienen estas estrategias de diseño (notificaciones constantes, likes, etc.) de las redes sociales en la salud mental de los niños, niñas y adolescentes?

Si pensamos en juzgar al internet por lo bueno o por lo malo no es así porque también a través del uso del internet los chicos tienen apoyo. ¿Cuántos adolescentes actualmente a través de un correo han alertado a las autoridades de una institución? Hay un video que se está circulando y que está vulnerando potencialmente a algunos de los compañeros. Si vamos más allá, varios chicos han encontrado en el uso de las redes sociales el poder vincularse en comunidades digitales y que les cuidan también. Entonces el twich, el youtube, son plataformas que también les permiten a ellos aspectos positivos. También hay cosas negativas. Por lo tanto, no se trata justamente de prohibir o decir que no se usen las redes sociales o cosas por el estilo, sino hablar con ellos sobre el uso saludable y adecuado de todos estos dispositivos. Así que, comparto contigo. Sería un error satanizar las redes sociales porque ¿Cuántos chicos muestran sus talentos a través de una plataforma? Están mostrando lo que han aprendido y hay gente que les apoya, que les brinda soporte. Y esto lo vinculamos a lo que habíamos conversado antes, es decir a los niños, niñas y adolescentes que no pueden acceder al mercado laboral, quizás las redes sociales les han permitido ganar cierta independencia porque cuando quieren conseguir algo a nivel laboral de la manera

tradicional quizás no la encuentran y han encontrado a través del internet un emprendimiento. Cómo no aplaudir la idea de que algún chico esté generando ingresos a sus 16, 17 años porque es muy bueno en el "Fifa" por ejemplo, o que sabe bailar, o sabe programar. Estas son las maneras en la que los niños, niñas y adolescentes también se revelan a esto de: "Cuando salgo del colegio tengo que ir a la universidad, tengo que trabajar" porque a veces ese no siempre es el plan. Así que, también se lo puede ver desde ese lado.

4. ¿Has notado diferencias de como los niños, niñas y adolescentes reaccionan emocionalmente a las interacciones en línea en comparación con las interacciones físicas? ¿Qué importancia tienen las interacciones físicas para el desarrollo de habilidades sociales y emocionales en los niños y niñas en la era digital?

Si partimos del hecho que las interacciones en línea o digitales no es que no son reales, evidentemente tienen un impacto en las personas, por eso los chicos, los más niños, niñas y adolescentes se enamoran de una persona que está al otro lado del mundo entonces evidentemente es real. Decir que es porque es a través del mundo digital no es válido sería un grave error, pero de igual manera yo pensaría que las redes sociales y el internet han ayudado a potencializar temas de las interacciones sociales en el mundo físico porque cuántas veces he escuchado historias de adolescentes que conocen a alguien a través de alguna plataforma, hablan y luego tienen un encuentro, quizás situaciones que sin el uso del internet no se podrían dar.

Creo que en este momento ambos tipos de interacción son necesarias para las personas y eso ha quedado demostrado totalmente en la pandemia, cuando la única forma de vinculación y acercamiento a las personas que teníamos era ese, y ahora sigue estando ahí, sigue presente y nadie puede negar que lo que sucede en esos espacios es válido, me genera emociones, sensaciones, opiniones, pensamientos. Entonces cuando los chicos tienen algún tema en línea, pelean en línea, al otro día llegan al colegio y siguen con el tema, es real. Es parte del mundo digital, el mundo físico está ahí, se necesitan los unos a los otros, están relacionados.

5. En el tema de Bullying ¿Son las mismas consecuencias hacer bullying por redes sociales que el bullying de manera física?

En el tema de las violencias tomando en consideración este caso que acabas de mencionar, el acoso digital definitivamente se transponla y están presentes, porque el adolescente que está siendo víctima de acoso escolar es muy probable que ese acoso siga en redes sociales y para la persona, el chico, el adolescente va a ser muy doloroso que estando en el recreo sus amigos le dejen jugando solo o estando en línea sus amigos le bloqueen o no le dejen ingresar al juego. O sea, las emociones que se generan son exactamente las mismas, el medio es el diferente. Quizá lo digital te permite a ti el anonimato. En este sentido, cuántos chicos se crean cuentas falsas para simplemente como dicen ellos "tirarle hate, funarle" desde el anonimato. Entonces este tema que te estoy dando ahorita en el caso del acoso escolar alguien se inventa un chisme, y no sabes quien fue o de donde salió, exactamente algo parecido pasa en el tema del internet; alguien dice cualquier cosa y no saben de dónde salió. Así que es totalmente extrapolable lo que pasa en línea y lo que pasa en el mundo físico. Se puede vivir de la misma manera. Quizás en el mundo digital es más complejo porque los chicos cambian el IP o buscan cualquier forma para no dejarse detectar. Y por ejemplo si vamos a cómo actúan las instancias legales entorno a esta situación quizás todavía está limitado. Sé que tienen sistemas y pueden buscar información, pero siempre redunda esto en el sistema público que cuando alguien hace una denuncia de esto o de violencia sexual, están rebasados y meses después se tiene una respuesta.

6. ¿Qué recomendaciones darías a los padres, educadores y cuidadores de los niños, niñas y adolescentes para bordar o prevenir los riesgos en la salud mental asociado al uso de redes sociales e internet?

Las recomendaciones que se pueden manejar en este sentido son por ejemplo limitar el uso de los dispositivos en la mayor medida y proveer a los niños y adolescentes otras opciones de entretenimiento. Ser un modelo, un ejemplo. Si padres y madres están comiendo y están con el celular ahí en la mesa, Quizás una buena manera en la que los adolescentes se puedan autoregular, yo como persona que estoy tomando un rol de cuidador enseño con el ejemplo. Los padres, madres, docentes que trabajan con adolescentes deben estar interesados de aprender del mundo digital. No sería entendible que de la manera en la nos estamos moviendo, que nosotros mismos como adultos hagamos que la brecha digital sea más grande entre nosotros mismos. También esa es nuestra responsabilidad para cuidar, conocer por ejemplo de control parental. En algún momento recuerdo haber hecho una charla, un taller para manejo informático del control parental, pero cuando vi que me decían "no puedo ingresar al zoom" no se puede llevar a cabo ese tipo de estrategias. Obviamente estar cuidando, estar presente en la vida de los chicos son cosas que ayudan. Pero por ejemplo ahora, padres y madres de familia lastimosamente tienen que estar fuera de los hogares trabajando, y eso precisamente complica mucho más el panorama de la supervisión. Estar enterados que sucede en redes sociales a través del tik tok principalmente circula mucha información, circulan retos, circulan noticias falsas y eso es lo que consumen los adolescentes.

Yo tengo bien clavado el tema de un colega que es psicólogo también y descubrí que él tiene una cuenta de tik tok y le dije: "cómo así tienes tik tok? Porque ya somos de otra generación y me respondió que quiere tener porque quiere saber más o menos que está en tendencia, que es lo que están consumiendo mis chicos, porque vale la pena para saber de dónde sacan las palabras que dicen, los chistes que hacen. Por ejemplo, Facebook ha quedado relegado para las personas más adultas en tanto que Instagram es más para chicos. Pero, es estar en esos espacios también, conocer esos espacios, saber cómo se mueven. Poner límites en cuanto al uso del internet. No puede ser posible que niños y niñas lleguen al colegio con el celular, por ejemplo. Eso les corresponde a las instituciones educativas, pero también a los padres. O que se vayan a dormir con el celular porque por eso también se altera el sueño, el estado de ánimo, los períodos de atención cambian, entonces hay que poner un orden, una regla en torno a eso.

Lo ideal es que los chicos empiecen a utilizar de manera autónoma el celular a partir de los 11 o 12 años con supervisión de los padres y de ahí poco a poco se les ha ir dando cada vez mayor independencia con el uso del celular, pero eso no es que llegan los 10 años y toma tu teléfono y tu verás como lo administras, que haces, esas cosas luego se convierten en problemas.

7. ¿Qué papel crees que deberían desempeñar las empresas de redes sociales, de internet y las autoridades gubernamentales para mitigar los impactos negativos en la salud mental de niños, niñas y adolescentes?

Yo pienso que lo ideal sería actuar con responsabilidad. El tema de la seguridad es utópico, es como pedirle al lobo que no se coma las ovejas, pero las riquezas de las empresas en torno a esto, como Amazon, es un ejemplo de cómo ha repuntado con el uso de información que ellos tienen disponibles. Pero es que es hipersalvaje el consumismo, el capitalismo, entonces como te digo, es utópico pedirle al lobo que sea responsable en esas situaciones. Entonces más que las empresas nosotros (las poblaciones, las comunidades, las organizaciones sociales), desde nuestros propios recursos, deben trabajar, deben unirse y un poco hacer frente a este tipo de situaciones que nos van vulnerando, que nos van dejando. Es tan brutal estas situaciones que a veces nos tienen tan metidos en estos temas del consumo a través del internet, de las redes

sociales, que simplemente no queda tiempo de hacer otra cosa más que pensar en el famoso que va a venir, en el tren que hay que hacer. Esto es lo que Jaime Breilh dice en la Determinación de la Salud Social en el sentido de que las personas, los colectivos tenemos uso de autonomía relativa que nos permite precisamente hacer frente a este tipo de situaciones cuando el sistema capitalista nos está consumando ahí es donde nosotros aparecemos. Realmente no sé qué tanta responsabilidad, qué tanta conciencia, qué tanta mentalidad de sustentabilidad, de seguridad, de salud, tengan estas empresas, pero si ellos no entran en esta lógica de las cosas que nosotros como colectivos necesitamos para vivir saludablemente, entonces pienso que la idea también es ir por eso, exigir cada vez más derechos, organizarnos, dar voz a los adolescentes, reconocer su capacidad de voz, entonces es eso.

El estado frente a estas situaciones debería hacer definitivamente que los niños, niñas y adolescentes, los adolescentes, la ciudadanía participe, o sea, no se puede conseguir una política pública sin que se dé una real participación a los niños, niñas y adolescentes, a los adolescentes. Simplemente se les instrumentaliza para decir que "está es una propuesta que se ha hecho con adolescentes", pero solamente se les pone ahí y siguen tomando las decisiones las mismas personas. Entonces hay que entrar en esa lógica también del adultocentrista, paternalista del estado. Si pensamos en esto vemos como niños, niñas y adolescentes y adolescentes no son tomados en cuenta en su capacidad de proponer, de incidir en las políticas porque simplemente es el mundo del adulto y lo mismo pasa con las personas adultas mayores, porque lo que más se valora es la posición del adulto por eso se desconoce lo que dicen los niños, los niños, niñas y adolescentes, pero hay que cambiar esas lógicas.

Es una propuesta desde la salud colectiva. Lo que debe tomarse en cuenta es la salud de los pueblos y como te digo, el punto que más luz nos da es la determinación social de la salud. O sea, básicamente significa que los procesos que nos enferman, como en el caso de la salud mental: no es una mente que está mal o sea que sus neo transmisores no funcionen, sino que hay determinantes sociales que van influyendo justamente en como una persona accede a la salud, al cuidado. Entonces frente a esto, están esos procesos que de alguna manera nos determinan por condiciones, pero ahí está el tema de la autonomía que cada persona, colectivo, organización, puede generar para hacerle frente a esto.

**Ola Bini**[491]

1. A tu consideración, ¿cuáles serían los principales riesgos para la privacidad de los niños, niñas y adolescentes en las redes sociales?

Los principales riesgos, en verdad empiezan muy temprano. Por ejemplo, lo que es muy común es que padres publiquen imágenes e información sobre sus hijos antes de que ellos puedan concienciar este uso, esto quiere decir que en el futuro tú ya vas a tener muchas imágenes en el internet que ya estaban antes de tu posibilidad de decisión. Entonces, estos derechos de privacidad de niños y niñas empiezan con los padres. Esto significa que ya existe información. Desde mi perspectiva, privacidad significa el derecho de controlar la información sobre ti, no significa esconderte, sino tener la potestad y la posibilidad de cuándo y a quienes revelas información, y qué tipo de información revelas. Por lo tanto, si los padres publican esta información sin que antes tú puedas hacer este discernimiento, es una violación de derechos a la privacidad. Ahora bien, esta información será utilizada quizás para entrenamiento de reconocimiento de emociones, y cada imagen que alguien publica sobre ti; cada texto, cada información, cada uno de estos, es violación. Los riesgos son grandes.

Por otra parte, oficialmente los niños no deberían utilizar redes sociales. Por ejemplo, Facebook tiene un mínimo de edad para ser utilizado, pero esto no es viable y hay muchas personas que utilizan las redes cuando tienen menos edad, pero las redes como negocio están utilizando esta información entonces tu estas revelando esta información muy temprano, y al mismo tiempo tenemos ejemplos en las escuelas sobre el uso de whatsapp como comunicación en clases. Pero whatsapp también es parte de "Meta", y al ser parte también hay un uso de información desde esta perspectiva de privacidad. Entonces un riesgo muy grande es que solo existiendo en la sociedad actual va a generar violaciones de tu privacidad y tú no tienes control sobre esto, es decir tu no vas a poder decir "no quiero estar en este grupo de wp de la escuela" porque es parte de la coordinación que hacen ellos. Por lo tanto, hay mucho de estas brechas que viene desde la perspectiva inconsciente de todas las partes, pero que genera violaciones.

2. ¿Cómo se relaciona la privacidad a la protección de datos personales?

En verdad son muy similares entre: protección de datos personales, ley de herramientas personales, etc, todas estas son maneras de proteger tu privacidad. Por ejemplo, en el caso de Ecuador la Ley de Protección de Datos Personales, da diferentes tipos de derechos para que puedas controlar tu información, entonces esto da derechos legales que ayuda a tu privacidad, pero el derecho de la privacidad y la intimidad es parte de la constitución, pero en la ley se da herramientas más específicas como se va a manejar y las responsabilidades que los custodiales cada uno tiene que cumplir con tus datos personales. Las herramientas son para protegerte y lo mismo pasa con la seguridad, mucha herramienta de seguridad en verdad da la posibilidad de controlar tu información, es como si tu utilizaras "cifrado" para comunicación. Cifrado es una herramienta de seguridad, pero si tú estás utilizando esto para controlar y asegurar que nadie más

[491] Ola Martin Gustafsson, es un desarrollador de software, programador y activista de Internet sueco. Desde 2013 reside en Ecuador, donde trabaja en el Centro de Autonomía Digital en temas relacionados con privacidad, seguridad y criptografía. En abril de 2019, fue detenido en Ecuador debido a su presunta vinculación con Julian Assange y Wikileaks. Su proceso penal continúa abierto. Su caso atrajo la atención internacional y planteó cuestiones sobre la libertad en línea y la protección de datos. Entrevistado el 01 de mayo de 2024.

que tu pueda leer un contenido, entonces de esta manera la privacidad utiliza herramientas de seguridad para generar la posibilidad de control.

3. Con respecto a la Ley de Protección de Datos Personales ¿aún no existe un superintendente cierto?

Si hay superintendente hace dos semanas, no recuerdo el nombre de él, pero justo hace una semana (el martes de la semana anterior) él fue ratificado por la Asamblea. Entonces ahora hay superintendente, pero no hay Superintendencia, tampoco hay presupuesto para la misma, y esto significa que aunque haya un superintendente no va a tener mucho poder hacer cosas hasta que haya presupuesto. Me parece bien que él esté hablando de algunos temas, pero todavía no tiene dientes.

4. La Ley Orgánica de Protección de Datos, en las disposiciones transitorias habla de que luego de dos años empezaría el proceso sancionatorio, pero pasaron dos años y no hay aún superintendencia. ¿Cómo podría esta institución estatal controlar, regular o garantizar el derecho a la protección de datos personales de los ecuatorianos? Considerando estas relaciones de poder bastante antagónicas entre las empresas de datos, redes sociales, etc., que muchas veces tienen más poder que los estados.

Sí, yo creo que esto va a ser muy difícil porque los centros de poder en el Ecuador son muy complicados y son vinculados entre ellos en una manera de que no es claro cómo puedes evitar. Lo más importante es, en teoría, ser independiente. Si puedes ser independiente esto va a generar la posibilidad, si tú tienes presupuesto y la posibilidad de hacer multas y sanciones, esto va a generar un poder, pero en práctica no va a ser independiente. Entonces yo creo que lo que vamos a ver ojalá, todavía va a sancionar, pero el problema es que siempre es como que tu sancionas una empresa, y también es la empresa del presidente, entonces como va a mantener su poder y la potestad en estas situaciones. Yo creo que vamos a hacer sanciones selectivas lastimosamente.
Una manera de manejar esto es que hay observación de medidas independientes sobre estas decisiones para demostrar cuando estas cosas pasan. Yo creo que lo más útil sería que la superintendencia sea muy transparente en todo lo que hace. Si yo soy superintendente, yo quisiera tener mucha transparencia para demostrar que no estoy haciendo cosas selectivamente, para demostrar que estoy sancionando de una manera objetiva.

5. Con respecto a los organismos internacionales. Se que hay un Convenio Iberoamericano de Protección de Datos, La ley Orgánica, pero ¿Existe algún organismo actualmente trabajando en un convenio internacional para regular este derecho en auge?

No, y lastimosamente es muy probable que no pase pronto, porque Estados Unidos tampoco tiene un acuerdo federal. Por ejemplo, hay una Ley en California que es muy buena, y desde hace 15 años EEUU han intentado proponer leyes federales, pero hasta donde yo sé, ellos no logran pasar los filtros. Y hasta EEUU tiene una ley de protección de datos personales va a ser difícil hacer algo muy internacional. Yo creo que lo más importante para ecuador, por ejemplo, estos acuerdos bilaterales muchas veces están basados en el comercio, entonces muchas veces no están enfocados en derechos sino en libre comercio. Así que desde esta perspectiva es difícil ver la propiedad intelectual y todas estas cosas. Yo creo que necesitamos nuevas iniciativas y necesitan ser regionales, entonces yo creo que Ecuador debería empezar con la región Alba, que no existe, pero empezar con Colombia, Perú, Chile, Argentina y Brasil para tener algo de América

Latina y esto va a generar suficiente fuerza para hacer acuerdos entre América Latina y Europa. Porque una de las cosas que el superintendente necesita definir son cuáles legislaciones son iguales a las de Ecuador para importe o exporte de datos, pero esto actualmente va a ser muy difícil como por ejemplo como vas a decir como no es seguro exportar datos a USA, pero desde una perspectiva legal esto es lo que necesita decir, pero desde una perspectiva de libre comercio va a ser un suicidio hacer esto. Yo creo que América Latina necesita un puesto un poquito más fuerte para hacer este tipo de negociaciones para proteger su información y los datos personales de sus ciudadanos.

6. Tengo entendido que la Ley Orgánica de Protección de Datos Personales tiene su base en RGPD y que la manera de proteger los datos personales en Europa es diferente a la americana, eso podría llegar a ser un problema aterrizando en el tema de redes sociales, no?

La verdad es que, si tiene su base en las reglamentaciones de Europa, pero lastimosamente sacaron todas las cosas importantes y agregaron aquí en Ecuador muchas excepciones, eso significa que hay muchas entidades que no necesitan en verdad cumplir con la ley de protección de datos personales, entonces esto va a generar más problemas desde la perspectiva de compatibilidad, pero al mismo tiempo porque esto es base en comercio es posible que solo van a ignorar todas las compatibilidades y decir que son compatibles, vamos a perder desde la perspectiva de derechos. Esta es mi perspectiva realista.

7. ¿Crees que la Ley Orgánica de Protección de Datos Personales es suficiente para proteger la privacidad de los niños, niñas y adolescentes en redes sociales?

¿De Ecuador?, No. De ninguna manera. Lo que es importante aquí es que hay una excepción grande y es que tú puedes ceder los derechos de la ley con un acuerdo, y todas las redes sociales tienen términos y condiciones y esto cumple siendo un acuerdo, entonces si tú tienes un sitio como Facebook sus términos y condiciones están ahí. Si tu utilizas Facebook estás haciendo un acurdo con Meta, tú dices que no tienes derechos, pero para utilizar esta red necesitas ceder tus derechos. Es por esta razón que la Ley de Protección de Datos no importa en este caso. En este caso los derechos son renunciables porque hay excepciones para renunciar. Si, los derechos son irrenunciables, pero las implicaciones de los derechos si son renunciables. Eso es lo que es muy triste con la ley actual, no tiene mucho poder.

8. ¿Cuál es tu opinión sobre la extracción constante de datos personales de ciudadanos ecuatorianos especialmente de niños, niñas y adolescentes por parte de grandes empresas de datos?

Yo creo que es un problema grande, creo que lo más probable es que es totalmente ilegal y creo que tendrá efectos grandes para los niños en el futuro, pero yo no sé cómo evitarlo porque estas empresas nunca van a ser sancionadas para este tipo de fuga de datos, entonces no tengo mucha esperanza. Es un problema grande y es una vibración grande de la seguridad y la privacidad de estos niños y adolescentes.

9. ¿Qué relaciones conflictivas y de poder identificas en el contexto de la explotación de datos personales de niños, niñas y adolescentes en Ecuador?

Yo creo que el conflicto grande va a ser justo entre comercio y derechos, y en general si es posible hacer muchas cosas sin explotar datos personales, pero no hay empresas que quieran

hacer cosas con respecto a los derechos. Estos son los puntos más grandes y el comercio siempre va a ganar. Antes que de se pase la ley pidieron comentarios de diferentes organizaciones sociales y cámaras de comercio y nosotros dimos comentarios de la ley, de cómo mejorarlo, pero la asamblea no aceptó ningún comentario de la sociedad civil, pero si de la cámara de comercio. La ley actual está basada mucho más en las necesidades del comercio que de la sociedad civil.

10. Hace un momento me comentabas que quitaron de la Ley Orgánica de Protección de Datos Personales temas importantes que si regula el RGPD. ¿Cuáles?

Lo más importante son las excepciones que agregaron, pero también hay esto del control algorítmico y el derecho de ser olvidado.

11. Actualmente, ¿cómo se podría garantizar la protección de datos personales? Considerando que no hay superintendencia y que la única vía regulada es el habeas data.

Si, desde una perspectiva didáctica, si tú tienes una vulneración a tus datos personales, siempre puede poner una denuncia administrativa basada directamente en la ley. Va a ser difícil y costoso hacerlo, pero como dices tú también tienes habeas data. Yo he hecho un habeas data y no fue muy exitoso. Todos metieron las entidades en mi caso. Entonces, en teoría habeas data debería funcionar, pero no hay muchos abogados en Ecuador que tengan experiencia con el habeas data y también es muy costoso hacerlo de esta manera, entonces en práctica es difícil garantizar los derechos. El primer paso, es solo intentar utilizar tus derechos: mandar un correo a una empresa, por ejemplo, yo hablé con un chico hace algunos días sobre enviar una carta a CNT o a Claro pidiendo información que tengan sobre mí, y solo pedir hasta ver los datos que tienen. Esto siempre es el primer paso, si ellos contestan quizás van a respetar los otros derechos mejor, pero si no contestan, por ejemplo, solo hay algo administrativo de habeas data.

Lo que es muy triste es que aquí en Ecuador… en otros países hay gremios para consumidores, por ejemplo, que a veces ellos pueden hacer casos colectivos contra empresas, por ejemplo. Porque el caso de una empresa grande que no tiene respeto a un cliente no van a tener respeto a miles de clientes, entonces en teoría tu deberías hacer algún tipo de recurso colectivo, pero en Ecuador no existen estas organizaciones que hacen este tipo de cosas, es decir demandas colectivas. Esto es algo que debería existir en Ecuador también. Si existe como figura legal en Ecuador, pero no existen organizaciones que en verdad hacen este tipo de controles para proteger consumidores o clientes.
En mi caso ha sido vigilancia contra mis abogados, contra mi persona también, entonces esto va a ser útil si llegamos a denunciar estas partes.

12. ¿Qué papel juegan las normativas y políticas existentes, si es que existe alguna, tanto a nivel nacional como a nivel internacional para la protección de datos personales y para la salud mental de los niños, niñas y adolescentes en Ecuador?

Desde la perspectiva de protección de datos personales tenemos la constitución, creo que es el artículo 66 de la constitución ecuatoriana del 2007 y simultáneamente tenemos la declaración de derechos humanos de las Naciones Unidas. Estas son las bases para la privacidad de datos personales, después hay otros reglamentos y otros acuerdos internacionales, pero estos son los dos grandes. Desde la perspectiva de salud mental para adolescentes y niños, niñas y adolescentes, no estoy muy atento de este lado. Entonces yo no sabría qué tipos de reglamentos o fundamentos hay. Yo creo que el derecho a la vida y a la salud son derechos humanos, entonces salud mental es parte de estos derechos humanos también.

13. ¿Cuál es tu percepción sobre la urgencia de generar normativas y políticas adecuadas en el Ecuador, en la región y en el mundo para abordar esta problemática?

Yo creo que estamos tarde, que todo el mundo está tarde y Ecuador es muy tarde con esto porque solo se puede ver la explotación de datos personales, las fugas que pasan, el ejemplo de Novaestrat que no recuerdo la data que fue, pero hubieron muchas fugas, las protecciones no son buenas, Banco del Pichincha, CNT, todo esto. Hemos visto muchas cosas, incluso por parte del gobierno. El gobierno filtró por error dos veces las personas con COVID en el Ecuador desde el Ministerio de Salud, entonces yo creo que también podemos ver desde la perspectiva de todas las llamadas para vender cosas que recibimos todo el tiempo. Entonces esto es un problema en Ecuador, ha sido un problema desde hace mucho tiempo. Creo que ya es muy tarde esperar para que haya una Superintendencia también y, no sé si va a ser posible para la superintendencia controlar la situación porque está esparcido por todas partes.

14. ¿Qué podrían hacer los padres para proteger el derecho a la privacidad y la protección de datos personales?

Primero, no publicar su información. No publicar imágenes. Cuidar y respetar la privacidad. Porque esto va a ser un problema en el futuro, hay muchas personas que roban datos personales de niños y niñas y utilizan para robar su identidad después. Entonces, esto es algo que ya pasa, este es el primer paso. El segundo paso, no sé si es práctico, pero en teoría niños y niñas no deberían utilizar redes sociales. En práctica quizás es imposible, pero por ejemplo en el caso de la escuela pensar en vez de tener whatsapp para el niño, el padre puede estar en estos grupos para evitar los problemas de privacidad para el niño y la niña.

15. ¿Cómo equilibrar el acceso a esta información con el derecho a la privacidad?

En verdad esto es algo que también las escuelas tienen mucha responsabilidad para buscar mejores formas que respeten la privacidad de los niños y niñas. Yo creo que muchos maestros no entienden el problema de utilizar WhatsApp para estas cosas, por ejemplo. Pero nosotros hemos visto incluso como maestros utilizan el acceso a WhatsApp para acoso sexual contra estudiantes y este tipo de cosas, porque tienen la posibilidad de comunicar en privado. Esta no debería ser la manera de hacer cosas, el maestro no debería tener acceso a una manera privada de contacto con niñas.

16. ¿Qué podrían hacer las empresas para garantizar el derecho a la privacidad?

Yo creo que la primera parte de esto es implementar protocolos para protección porque muchas empresas no tienen medidas de seguridad actualmente y este es el primer paso, en verdad proteger la información. O bueno, quizás el primer paso sería no tener información que no sea necesario. Muchas empresas en Ecuador recolectan información que no necesitan, y esto es algo que genera que tengan más información. Entonces la primera medida de seguridad es no tener la información, y la segunda es proteger de una manera suficiente esa información.
Hasta que tengamos una superintendencia, necesitamos esperar que las empresas auto verifiquen y auto controlen. Esto va a ser difícil, pero las empresas necesitan tomar su auto responsabilidad y como consumidores nosotros deberíamos pedir a ellos que respeten esto, y utilizar otras empresas si no podemos confiar en las empresas que tenemos.

17. Hemos estado hablando del derecho a la privacidad y protección de datos, y aquí se vincula otro dato más que es el derecho a los consumidores. ¿Cómo podemos hacer frente a estas grandes empresas?

Todos estos derechos digitales en realidad están vinculados juntos y es difícil muchas veces separar los derechos de seguridad, privacidad, derecho del consumidor, derecho a la libre expresión, todos estos derechos son casi lo mismo. Yo creo que necesitamos pedir a los asambleístas que regulen las empresas grandes porque como hemos visto en Estados Unidos, por ejemplo, los monopolios son difíciles de controlar, pero si es posible. Estados Unidos actualmente está trabajando contra Google para ver si pueden controlar. En Europa están controlando a Apple para mejorar la situación contra estas empresas grandes. Es algo que, en teoría, el gobierno de Ecuador también debería intentar aquí contra las empresas. Pero otra vez, va a ser difícil cuando Noboa está vinculado con una de las empresas más grandes. Entonces, la decisión electoral también es importante en esta parte. No podemos elegir personas tan vinculadas a estas empresas.

18. Ahí me surge este tema de los modelos, ¿no?. El modelo americano es: capitalista y, las empresas, como se ha demostrado, llegan a tener más poder que los mismos estados. Mientras que, en el modelo chino, es el estado tiene la información que deben tener las empresas. ¿Qué opinas de esto? ¿Cuál es la alternativa, el europeo?

Hay problemas con los dos modelos. Desde mi perspectiva política yo no soy muy fan del capitalismo en general entonces mi alternativa sería más como cooperativos. Es decir, cooperando entre ellos. Quizás no es muy práctico, pero sí, el modelo europeo creo que es el mejor, pero hay problemas allá también, entonces no sé. Yo creo que si tú tienes un modelo autoritario de estilo chino no es muy bueno, pero los modelos de oligarquías de Estados Unidos, es malo de otra manera. Los derechos colectivos son muy importantes en una población. Cada uno de estos modelos tiene diferente fuerza en los diferentes derechos, pero yo creo que lo que pasa en Occidente es que los derechos colectivos tienen una fuerza muy grande.

19. ¿Qué modelo sería el adecuado para desarrollar el derecho a la privacidad?

No sé, en verdad. Yo creo que primero el modelo de cómo manejar nuestros datos si no puede funcionar debería ser el indicador. Creo que una de las cosas que pasa muchas veces es que, hay mucha oscuridad, muchas cosas escondidas Entonces, si entendiéramos como están utilizando nuestros datos, si hacemos la transacción consciente, desde una perspectiva capitalista en general, para tener un mercado libre capitalista todos los actores deberían tener la misma información. Esto es uno de los fundamentos del capitalismo, porque solo con toda la información tu puedes generar precios correctos en el mercado, pero lo que pasa con datos informáticos es que el valor de los datos y como están utilizando, es información que está escondida a nosotros, desde la perspectiva de explotación. No sabemos qué tan valiosa es nuestra información y no sabemos cómo están utilizando las redes sociales esta información. Y por esta razón, no valoramos nuestros datos, y esto significa desde una perspectiva capitalista, no hay una igualdad de actores.

20. En derechos colectivos, de pueblos y nacionalidades indígenas, existe el derecho que se llama la consulta previa, libre e informada. Es decir que si vas a tomar decisiones sobre temas que me pueden afectar, deberías preguntarme y buscar mi consentimiento, de manera previa, de manera libre e informada para poder dar una respuesta, ¿qué opinas?

En verdad esto es algo que dice la Ley de Orgánica de Protección de Datos Personales, y no solo de que sea una consulta previa e informada, sino que esto de la especificidad es algo que

muchas veces falta también. Es como que "vamos a recolectar los datos para hacer todas estas cosas", esto no es específico.

Tú puedes pensar en la pregunta de si en verdad un adolescente o un niño puede formar un acuerdo, porque un acuerdo necesita suficiente nivel de desarrollo mental y toda esto para entender las consecuencias. Entonces desde esta perspectiva, yo diría que quizás no es posible para un adolescente hacer este tipo de cosas informadas, porque no es posible informarles. Si tú tienes una persona que tiene 10 años o 11 años por ejemplo, ¿puedes en verdad asegurarte de que ellos o ellas entiendan?, quizás no es posible. Y esto significa que quizás no puedes tu tomar decisiones sobre ellos o ellas.

21. ¿Qué podría hacer el estado para garantizar el derecho a la privacidad?

Presupuesto para la superintendencia, regresión de la ley, y para que la superintendencia haga un trabajo bien hecho, asegurar la independencia de las diferentes partes del gobierno; incluso entre el gobierno y empresas grandes. Cooperación internacional también. Necesitas una ley que tenga suficiente poder, pero los comercios no quieren esto.

La privacidad digital es muy importante justo por la vinculación de los otros derechos, y si podemos proteger el derecho a la privacidad esto significa proteger los otros derechos digitales también, y no podemos pensar solo en los derechos actuales, también necesitamos pensar en los niños, niñas y adolescentes porque ellos tienen derechos cuando son adultos, y no podemos violar los derechos ahora para que después ellos se van a dar de cuenta cuando sean adultos que ya violaron sus derechos.

**Lorena Naranjo**[492]

1. ¿De acuerdo a su experiencia, cuáles son los principales riesgos para la privacidad y la Protección de Datos personales de los niños, niñas y adolescentes en internet y redes sociales?

Ok, vamos a distinguir: en el Ecuador el derecho a la privacidad que deviene del artículo 12 del de la declaración de Derechos Humanos que habla de la vida privada, y nuestro parangón o nuestro equivalente es el derecho a la intimidad, por lo tanto, la estructura correcta es derecho a la intimidad o la mención correcta es derecho a la intimidad.

El Derecho a la Protección de Datos personales tiene otro contenido, ya no es la vida privada o lo que se busca resguardar en el entorno privado, sino la autodeterminación informativa, la toma de decisión sobre los contenidos. Los datos que tienes y los responsables de tratamiento: empresas, plataformas, etcétera. ¿Con cuáles son los lineamientos, obligaciones, principios y derechos que deben garantizar? Partiendo de esta distinción conceptual, vamos a decir que hay una serie de circunstancias que pueden verse afectadas respecto de niños, niñas y adolescentes.

En un primer plano, la intimidad de sus niños, niños y adolescentes que puede ser afectada incluso por sus propios padres. Debido a que existe una práctica que se llama sharenting, en donde hay un ejercicio de sobre exposición de los chicos. En el que los padres se encargan de subir fotografías, anécdotas, lugares de referencias, etcétera de niños, niños y adolescentes, en su afán de ser muy orgullosos y de exhibir los logros, los avances de los chicos y el riesgo evidente en eso es que existen fotografías que pueden o contenidos en general: videos, menciones, etcétera que pueden ser usadas para acercarse a estos chicos cuando estén en manos de personas inescrupulosas, eso es un riesgo de seguridad, de vida, de seguridad integral, de seguridad en respecto de su intimidad sexual. O también puede haber a través de sus contenidos la posibilidad de que otras personas puedan usarlos para hacer bullying, o cyber bullying. En este caso esta sobreexposición plantea esos posibles riegos.

También respecto de la intimidad, esta puede ser afectada por la exposición que hagan terceros pares de esos niños, niñas y adolescentes que tengan acceso a redes sociales, sobre todo porque es un compañero de aula y decides subir una fotografía en la que está tu compañero y si esa fotografía nuevamente te pone un riesgo de seguridad o te pone en un riesgo de sufrir algún tipo de acoso, violencia o cyberbullying. Y la que tú misma te puedes o tú mismo te puedes autogenerar como niño o niña de adolescente, y es cuando, por ejemplo, en el caso del niño se te ha habilitado muy temprano el uso de redes sociales, careces de los conocimientos mínimos y lo

[492] Lorena Naranjo Godoy, con más de 20 años de experiencia en el área. PhD. cum lauden en Ciencias Jurídicas y Políticas y Máster en Derecho de Nuevas Tecnologías por la Universidad Pablo de Olavide, en Sevilla-España. Investigadora, consultora BID y docente de pregrado y postgrado, autora de varios artículos académicos y conferencista nacional e internacional. Implementadora líder en empresas nacionales e internacionales, bancos y otras entidades del sector financiero, plataformas digitales, e-commerce en la adopción de modelos de protección de datos personales, seguridad cibernética y transformación digital incorporando Big Data, internet de las cosas, inteligencia artificial, con experiencia en el sector público y privado. Autora y líder del proceso de aprobación de la Ley de Protección de Datos Personales para el Ecuador y de otras normas que permitieron su implementación en el Sistema Nacional de Registro de Datos Públicos cuando fue Directora Nacional de DINARDAP. Ejerció como Directora de la Escuela de Derecho de la UDLA, Subsecretaria de Desarrollo Normativo del Ministerio de Justicia, Derechos Humanos y Cultos; asesora de la Presidencia de la Corte Nacional de Justicia y Directora Nacional de la Dirección de Registro de Datos Públicos. Actualmente, es directora de la Maestría en Derecho Digital e Innovación con mención en economía, confianza y transformación digital de la UDLA y Directora del Área de Derecho Digital y Protección de Datos Personales del Estudio Jurídico Spingarn. Entrevistada el 22 de mayo de 2024.

que haces es tú mismo publicar información de carácter íntimo o ni siquiera de carácter íntimo, sino incluso de cualquier tipo de información y tú mismo estás poniéndote en una situación de riesgo. Frente a estas dos situaciones que son violencia, tu propia seguridad o la situación de acosos o tipos de violencia, ¿no es cierto? Tenemos entonces todo este aspecto desde el punto de vista de la intimidad.

Desde el punto de vista de la protección datos personales. Los datos de niños, niñas y adolescentes entienden datos sensibles y por lo tanto, las empresas, cualquiera que estas sean, que manejen datos de niños, niñas y adolescentes deben tener lo que se llama un Marco de Protección reforzada, es decir sus principios, obligaciones y garantía de derechos deben tener unos lineamientos mucho más fuertes. Por ejemplo, un consentimiento explícito. En el caso de niños, ese consentimiento tiene que provenir de los padres y en el caso de los adolescentes, el consentimiento puede provenir de los adolescentes que superen los 15 años. De menos siempre van a tener que ser adolescentes que también requerirán la autorización de sus padres para el tratamiento de datos personales por esta condición de doble protección, por su situación de vulnerabilidad.

¿Qué significa que entonces hay una serie de prerrogativas, una serie de condicionamientos para el tratamiento de datos personales para niños, niñas y adolescentes? El consentimiento tiene que ser explícito. Tienes que hacer análisis de riesgos y evaluación de impactos y establecimiento de medidas de control de mitigación para disminuir los riesgos del tratamiento, si es que decides hacer tratamiento de niños, niñas y adolescentes, de datos de niños, niñas de adolescentes, porque tienes un deber de cuidado mayor y a su vez, necesitas también tener en cuenta que para procesos de valoración automatizada este está prohibida a menos que tú puedas tener alguna habilitación que te permita hacer valoraciones automatizadas. Esto en Cristiano es que no es posible hacer perfilamiento de niños, niñas y adolescentes sin una justificación, una base legitimadora, una habilitación legal.

¿Es un sistema preventivo o un sistema reactivo? A eso me refiero entonces, en el sistema preventivo tú construyes las reglas para evitar; en el sistema reactivo tú indemnizas cuando los daños ya fueron ocurridos y en Estados Unidos se llama Privacy que es el equivalente a privacidad, porque para ellos es un derecho del consumidor, mientras que para nosotros es un derecho fundamental y ellos tienen la distinción entre derecho del consumidor y derecho fundamental, porque ellos, de hecho, su Constitución no la han tocado desde su emisión.

Y el tema es que la diferencia conceptual de ellos, como ya debe saber, es que el para que tú seas o tengas un derecho al consumidor, debes tener la calidad del consumidor, debes ser parte de una plataforma, parte de tu servicio, etcétera, etcétera, mientras que para nosotros basta con tu sola existencia ser considerado ser humano, tú ya tienes de forma intrínseca a tú nacimiento de identidad, a tu propia existencia, el derecho fundamental a la intimidad, y a la Protección de Datos personales. Y esa es la distinción.

2. La Ley Orgánica de Protección de Datos personales manifiesta esta seguridad reforzada a los niños y niñas adolescentes, este consentimiento de no automatizar los datos. ¿Pero existen políticas o existen estas normativas? ¿En verdad se garantiza la Protección de Datos personales con respecto a redes sociales? ¿Puede garantizar esta protección a los niños, niñas y adolescentes frente a empresas como: *Meta, Amazon*, etc., ¿Qué tan garantista puede llegar a ser esto, existe una verdadera protección más allá de la ley?

OK te voy a contar lo siguiente. Efectivamente, América Latina no tiene el poder que tiene Europa para enfrentar a las grandes plataformas, porque Europa sí logra hacer estos ejercicios de contrapoder, mientras que América latina, como no está organizada, tiene que

hacerlo de forma empírica. Le voy a explicar cómo hay un caso famoso que, ojalá lo pudieras encontrar y si lo encuentras me ayudarías un montón porque yo no he tenido tiempo para investigarlo, pero que lo supe de boca de las autoridades para poder coordinarse. Las autoridades de Protección de Datos en América Latina lo que hacen es, como ellos se conocen porque son parte de una red iberoamericana de autoridades de Protección de Datos que tienen cada año unas reuniones y son amigos porque ya se convoca y se reúnen literalmente se llaman, se mandan whatsapitos, se llaman por teléfono y dicen, OK, hay una situación con una aplicación o con un uso inadecuado de la plataforma Tik Tok Por eso te digo, yo no he tenido chance de ir a revisar esto que te estoy contando, lo que te estoy contando es exclusivamente referencial porque me contó un amigo que era director de una entidad de estas que te cuento que era un súper intendente de protección de datos de su país y nos dice "Miren, está pasando esto, nosotros vamos a iniciar un proceso de investigación contra tiktok. Les vamos a avisar a ustedes para que hagan lo mismo y de forma empírica, sin que exista un convenio sin que exista un tratado sin que exista nada. Todos estos países se alinean para iniciarle la misma acción desde sus propias normativas locales, porque una de las características de la ley de Protección de Datos es que es de las pocas que es extraterritorial.

Igual que la RGPD, nuestra ley de Protección de Datos también tiene esa característica. ¿Ya entonces qué nos faltaba aquí a nosotros? Una autoridad que entre en este juego que te estoy contando de contrapoder ¿me explico? porque no es que hay algo articulado, ya te digo es muy pragmático. Pero bajo esta estructura tú logras hacer que tiktok diga "Ah chuta manguitas tengo que corregir el efecto práctico que nos pasó aquí en el Ecuador" es que yo trabajaba en estudio jurídico y me mandaron una pregunta de título, si es que esto que ya les estaba pasando en América latina también podría pasarles aquí en virtud de que nosotros ya teníamos una ley aprobada y yo les contesté, efectivamente te puede llegar a pasar no ahorita, pero no teníamos autoridad. ¿Pero qué es lo que pasa con tiktok? Dice: "A la mierda güey está bien entonces en estos países que protestaron y en este que, aunque no protestó, ya tiene una normativa que me lo va a prohibir, yo no voy a hacer eso."

Pero en los otros lo sigue haciendo. Y, por eso es que los europeos y todos los demás se quejan porque dicen que hay ciudadanos de primera y ciudadanos de segunda y los ciudadanos de segunda son los que no tienen ley para proteger. Y, por eso la necesidad de que haya leyes mucho más de que hay autoridad y que esta autoridad esté trabajando muchísimo más de que haya acuerdos, convenios, tratados, la figura que le quieras dar para que toda América Latina respecto de estos temas pueda trabajar al unísono y. ¿Como hacia Europa? ¿Pero esos son el deber ser hacia dónde tenemos que caminar? No son suficientes porque localmente careces de la fuerza. Tiene que ser en grupo.

Ya y además, localmente puedes iniciar una acción, te va a armar bronca, va a protestar, etcétera, pero la forma en la que encontraba Latinoamérica para tratar de medio organizarse de poder lograrlo es de esta forma, como te digo muy empírica. Y ubícate en los países que no tienen ley, que son Venezuela, que son Bolivia. Y, Paraguay. Esos pobres están en menos todavía. No tienes ni ley porque al menos nosotros por tener ley dijeron Ah OK no nos vamos a meter ahí.

Al menos en este caso puntual que te estoy comentando, decidieron hacer esto ahora en otros casos de otras plataformas que también consultaron como es la ley, etcétera, etcétera. Como ellos saben, lo que significa tener una normativa con sanciones, etcétera fueron los primeritos en cumplir, yo cuando salí de directora nacional y fui a trabajar en un estudio jurídico, yo me dediqué a contestar estos oficios, sólo para que tú sepas. Yo me dediqué a contestarle y decirle cómo se aplica todo, porque ellos son los que más saben y los que más, porque ya han implementado todas estas medidas de seguridad, de protección a otros lados y solo es cuestión de traspasarlas. Ya es el problema con los otros, con la con los chinos, con las plataformas del Asia, esos son los

realmente riesgosos y esos están en juegos, sobre todo para temas de niños, niños de adolescentes en juegos en línea.

¿O sea, qué los riesgos que tú estás mapeando en redes sociales? De todas maneras, Facebook trabaja un montón con Instagram, con whatsapp, etcétera para ser políticamente correcto. Las otras que son *tiktok,* que son *wechat*, que son todos los plataformas de juegos en línea no les importa nada.

Otras chinas japonesas pensé que allá hay normativas de Protección de Datos, tú vas a ver que esas normativas más bien tienen un sentido de vigilancia de la información de la población, más que un sentido de protección de derechos de los titulares.

Además, es duro pelearse contra ellos. Y si tú te fijas el caso descollante no fue contra Facebook, no es contra el *tiktok*.

3. Pero también lo que me hace entender es la urgencia de crear un convenio internacional al respecto, ¿no?

Sí. Bueno, no sé si ustedes están al tanto, pero hay, hay un caso reciencito que salió en la Corte Interamericana de Derechos Humanos, que se llama Cajar versus Colombia, donde se reconoce por primera vez el derecho a la Protección de Datos de mi sistema interamericano, sí.

Ahí dice que la mamá del derecho a la Protección de Datos es la intimidad, pero después terminas reconociendo un contenido esencial distinto y por eso es que son dos derechos diferentes. En la preconstitución. Y ese es el avance de esta resolución, el hecho de que no le dices que es parte del contenido de la intimidad, sino que le estás reconociendo un derecho autónomo independiente con contenido especial propio.

¿Por qué? Porque en ese pinchar de celulares no solo tienes un derecho afectado, tienes dos, el primer derecho es intimidad y el segundo derecho es Protección de Datos. La misma acción puede afectar dos derechos simultáneamente.

4. ¿Ya y ahora con respecto al modelo de negocio de las empresas de internet y redes sociales, que es básicamente la extracción de datos, y muy probablemente la comercialización de estos sin el consentimiento de los consumidores? ¿Cómo se podría proteger?

A ver ahí hay que distinguir nuevamente estamos seguros de que no hay consentimiento porque incluso hay consentimiento informado.

Yo a mi hija, por ejemplo, cuando le bajaba roblox porque yo tengo un montón de controles en las plataformas y en los iPads y a todo de mi hija y de mis hijos en general. ¿Qué es lo que me parecía? Me decían mami, no puedo pasar aquí, no me puedo bajar roblox porque dice que tú como adulto tienes que aceptar los términos y condiciones y leerte los términos y condiciones y decir que estás de acuerdo con que me van a hacer perfilamientos. Entonces yo que sé del tema me leía, decía bueno está bien, ya te acepto. El resto de papás. Olvídate no haces entonces hay un problema de falta de formación en padres sobre estos temas hay un problema de falta de empoderamiento de derechos, porque estos consentimientos los tienen.

5. Ya, pero es que más allá de eso, a ver dos temas, primero con lo justo que podría llegar a ser tener que entregar todos tus datos para acceder a Internet, que incluso ya está siendo considerado como un derecho humano. Y segundo, el tema del consentimiento informado, entendiendo que estos perfilamientos y demás los hacen algoritmos súper complicados que ni siquiera las personas que los programan pueden llegar a entender sus

resultados. ¿Entonces, de qué de qué consentimiento informado estamos hablando, si no puedes ni siquiera explicar lo que lo que está pasando.

Correcto, si estás cuestionando el modelo y es que esta forma en la que tradicionalmente se ha obtenido el consentimiento está en crisis. Ese es tu argumento porque es verdad, está en crisis, pero legalmente hablando. Incluso desde el RGPD, que es el modelo de estándar más alto en el mundo. Eso es lo que hay entonces, ellos a nivel legal están cumpliendo. ¿Que te cuestiones tú si es estándar legal es suficiente? Esa es tu tesis. Para saber si efectivamente con eso estás dando la garantía que requieres porque la ley, eso es lo que te pide. Si es que tu cuestionas eso vas a tener que sustentar cómo estableces una posible solución, porque no es solo establecer el cuestionamiento, sino como tú garantizas que efectivamente hay un mejor mecanismo que este consentimiento de padres que el mejor mecanismo sea trabajar en empoderamiento y en prevención y educación. OK.

Tal vez el mejor mecanismo sea otro tipo de consentimiento u otra forma de aproximación, pero lo que no puedes es hacer o lo que no va a funcionar nunca es la prohibición. ¿A qué me refiero con eso? Si tú llegas a decir, no puedes hacer tratamiento de adolescentes, no puedes hacer tratamiento de niños, no puedes hacer perfilamientos. Lo que va a ocurrir es una contracultura. Yo ya le veo a mi hija adolescente diciéndome que no puede acceder a redes sociales o a roblox, eso no va a pasar, y lo único que vas a establecer es un sistema de desprotección. ¿Entonces? Eso es parte de lo que te tienes que plantear.

6. ¿O sea, el Internet es entendido como como un derecho, como un acceso a la información, a conectarse, pero, sin embargo, quiénes son los dueños del mismo y para qué lo usan? ¿Y cómo estás prácticamente obligado a consentir entregar tus datos para poder acceder a algo que se entiende que llega a ser de todos?

Un derecho, o sea, creo que estás confundido a ver vamos por partes. El acceso a internet necesita de 2 elementos, dispositivos y conectividad, entonces para el acceso a internet significa en consecuencia que tú puedes navegar por cualquier buscador, acceder a cualquier servicio o plataforma *Windows, Google*, estos mismos videoconferencia, etcétera, etcétera. O redes sociales. El derecho de acceso al Internet no es derecho de acceso a una plataforma. Es el derecho que tenemos todas las personas de poder contar con los dispositivos y con los accesos para poder llegar, entonces el equivalente es al agua al agua potable para yo tener derecho al agua potable, necesito los cables y las tuberías y necesito que mi municipio de la localidad establezca un mecanismo eficiente con el cual yo puedo pagar mensualmente y acceder.

¿Me explico?, entonces no hay que confundir el acceso a dispositivos y a Internet como conexión IP, cualquiera de estos con el acceso a los servicios y plataformas, por ejemplo en *Google*, que es el buscador, tú no tienes términos ni condiciones, no tienes políticas de predicción de datos para el acceso está el buscador, ahí es la forma en la que ingresas a Internet ya, pero no necesariamente es la forma. También puedes simplemente colocar arriba WWW. Edu punto c. Y sobre la base de la dirección, el nombre de dominio, entras a Internet y tampoco hay en ese espacio ni unos términos y condiciones ni una política, porque eso es Internet. El acceso a la gran biblioteca virtual ya, pero para poder acceder a eso necesitas dispositivos y tu conexión IP habilitada porque le estás pagando a un proveedor.

Otra cosa es meterte en un software y una plataforma; en el software, en la plataforma que puede ser una red social que puede ser *Windows*, que puede ser un juego en línea, etcétera, etcétera. Si quieres usar eso sí, te aparecen políticas de Protección de Datos y términos. Quiero acceder a un ecommerce a *Amazon para* poder acceder si necesitas esto, y eso ya es otro ámbito, y en ese ámbito hay grandes plataformas, grandes propietarios, etcétera, etcétera.

7. Pero para buscar en Google igual se guardan tus datos, o sea, igual tienes un perfil

Y Google vive de eso. Entonces, entonces si vas a cuestionar la forma en la que está organizado Internet, tienes que establecer cuál es el límite entre el acceso y la posibilidad de que estos buscadores o que estos… porque no solo hay Google, hay Bing hay Yahoo; lo que sea ya, cómo, ¿cómo yo puedo acceder? Decido prescindir de estos, OK, me voy directamente con el nombre de dominio desde la parte de arriba, www.en edge. Pero eso, esa perspectiva es la que tú tienes que decir, OK, no quiero que me perfilen, no quiero que me revisen. Usa Firefox y si usas Firefox que ahí hay un dominio, hay una opción en la que te dice quiero permanecer anónimo, no me sigas Ah OK, hace falta difundir que esa opción hay en Firefox. ¿Las sabías no las sabías? Entonces no es que no exista, lo que pasa es que no hay el conocimiento o las habilidades de las personas para saber cómo hacerlo, y eso es distinto el derecho de acceso a internet, Ya te digo que es un derecho que te garantiza el Estado al decirte igualito que el agua potable. Porque el agua potable nos llega a la punta del Chimborazo, nadie vive ahí.

Llega a donde existe una población en la que el Estado puede hacer sustentable el acceso a dispositivos que en el caso del agua son las tuberías y al acceso. En el caso de Internet es la conexión a Internet.

8. Ya. Una cosa es entrar y otra usar un servicio de Internet, que no es diferente a usar un servicio en la vida real.

Y ojo, nuestro derecho en nuestra Constitución no habla de derecho a internet, habla del derecho de acceso a las tecnologías de la información y comunicación. Nosotros no tenemos derecho a Internet como sí tiene Europa.

9. Ya. Sería como entrar al Quicentro. Puedes entrar, pero si quieres algo toca pagar. ¿Y pagar es pagar con tus datos?
   En un caso, porque en otros. Te cobran.

10. Pero también se toman tus datos, o sea, les pagan, les pagan dos veces.

Claro, claro que sí, porque te pueden cobrar, pero por ejemplo en *Adobe Acrobat* tú puedes decir no, no quiero, pero te están cobrando por el PDF, por la firma electrónica, etcétera, etcétera.

11. Muchas gracias, Lorena, cuénteme por favor, de acuerdo con su experiencia. ¿Qué estrategias pueden implementar los padres y el Estado para promover una relación saludable y segura con la tecnología, protegiendo así la privacidad y la salud mental de los niños, niñas y adolescentes?

A ver. No privacidad, intimidad, Protección de Datos y salud. De acuerdo. A ver, creo que hay que ver que respecto de esto hay una suerte de multistakeholders, ¿igualito a lo que pasa con todos los temas de internet? ¿Qué quiere decir que todo el ecosistema es corresponsable? No es responsabilidad exclusiva de los padres, por eso es que la legislación establece regímenes de protección adicionales.

Para niños, niñas, adolescentes, voy a explicar, el Estado tiene que garantizar esto a través del derecho a la educación digital que está en el artículo 30 de la Ley Orgánica de Protección de Datos personales, si no me falla la memoria.

Los padres de familia tienen que hacer un deber de cuidado respecto de cómo los hijos manejan todas estas tecnologías y para eso tienen que hacer un ejercicio de concientización, de formación y de transmisión de valores a los hijos. Pero cómo haces eso si carecen de los

conocimientos, entonces hay un deber del Estado de hacer también ese proceso de empoderamiento y conocimiento a los padres que son los cuidadores de esos niños.

Asimismo, tienes a los colegios que tienen que garantizar la educación digital para garantizar eso formas a padres y formas a niños, niñas y adolescentes. Las empresas tienen que hacer procesos de capacitación, así, deben capacitar a los papás, formarlos para que tengan los conocimientos para poder transmitirlos a sus hijos. Finalmente, las universidades tenemos que formar profesionales que comiencen a entender estos temas y comiencen a discutirlos. Prueba de ello es que tú estando en una maestría que es de otra cosa, terminas aproximándote a estos temas.

Tienen que motivarse líneas de investigación. Los profesores deben tener formación específica en estos temas, es decir, todo el ecosistema. No se hace nada si sólo es responsabilidad de los padres, no hace nada y finalmente las plataformas, las plataformas tienen que todo el tiempo está retroalimentándose de la realidad. ¿Para qué? Para que vayan diseñando mecanismos de protección.

Ejemplo: lo que se llama control de foros. No había eso, es de recién y es de recién por las presiones que ha habido para la garantía de los derechos, especialmente por las autoridades de datos, porque esto no ha venido ni del sistema judicial tradicional ni de los tratados internacionales. Son las reclamos que están haciendo las agencias de Protección de Datos personales del mundo que suben el estándar de protección y que por un efecto replicador terminan aceptando otros ¿por qué? Porque saben que es un estándar de protección y prefieren asumir la responsabilidad de hacerlo de buena fe. Por eso si tú te fijas esos sistemas de reportar, los tienes en *Instagram,* los tienes en *Meta*. ¿Si haces una investigación de los juegos en línea de las plataformas chinas? No hay.

12. Me llama mucho la atención este tema. En la región. El RGPD y la Ley Orgánica lo llama responsabilidad proactiva, que es básicamente esperar que de buena gente la empresa se auto ponga reglas, es como sí poner al ratón, cuidar del queso

Al contrario, verás en la versión anterior de la directiva porque esta es una práctica de los modelos autorriesgo. ¿Todos, pero en la versión anterior lo que hacías es tu cumples esto? Esto es este otro y te entiende que tú has satisfecho tu obligación porque cumples el mínimo y con eso te lavas las manos. Lo que haces con el sistema de responsabilidad proactiva es qué inviertes reinviertes la postura. ¿Por qué? Porque el responsable de tratamiento debe demostrar que ha ido más allá de la diligencia debida y que entonces no me conformo con cumplir los mínimos, sino que sabiendo yo el estado de avance de mi técnica. Yo me autoimpongo medidas superiores de protección. Y por eso logró demostrarte que sí me vulneraron, sí me afectaron, etcétera, yo he actuado de buena fe porque yo estoy un pasito más. ¿Por qué se invirtió esto? Porque las plataformas en general y ahí no hablamos solo de redes sociales, sino en general. ¿Qué es lo que te decían? Uso la ISO 27000. La UVI en 27700 aquí dice que tengo que hacer esto, esto y un *checklist* yo ya hice a mí no me puede multar porque yo ya cumplí, no porque sobre todo con lo que son tecnologías emergentes, inteligencia artificial y todas estas que ya tienen mayores complejidades. Yo no me puedo limitar a un *checklist* porque solo yo sé lo que estoy haciendo con estos algoritmos complejos que tú estás mencionando con esas cosas. Entonces ese *checklist* me va a quedar cortito. En cambio, si te impongo a ti que me demuestres que hiciste más allá traslado, eso se llama trasladar o reinvertir la carga de la responsabilidad y de la prueba para que seas tú el que me tengas que convencer a mí de que hiciste lo suficiente.

13. ¿Ya siguiendo con la con las preguntas, cómo pueden las empresas de tecnología y redes sociales ajustar sus políticas?

Bueno, un poco estamos hablando de esto, no de la responsabilidad proactiva. O sea, mira, tienes que revisar de dónde viene la empresa si la empresa es americana o es de Canadá o es de cualquier país de anglosajón. Ellos tienen que adaptarse para cumplir en el Ecuador al modelo ecuatoriano y nosotros nos parecemos mucho al de Europa.

Y si quieres eso ya te digo, es lo que yo me dedicaba a trabajar la. Los primeros meses que salí de la Función Pública, OK, yo ofrezco productos y servicios en Ecuador que me falta en mi política para completar, me falta esto, este otro, pero no solo es completar la política porque las políticas no deben ser documentos meramente declarativos, sino que una vez que identificas la brecha que tienes que completar, tienes que volver la práctica en la organización, sino que existe.

Te voy a dar un ejemplo, ya supongamos que tu brecha sea que aquí en el Ecuador está prohibido hacer perfilamiento de niños sin consentimiento del titular, entonces nosotros en la política dirá solo haremos consentimiento, cómo se llama perfilamientos con autorización debido de los padres que serán previamente bla bla bla yo te pongo letra. ¿Pero la organización al interno tiene que saber que eso que se está declarando se tiene que cumplir y cómo va a tener que cumplir? Van a tener que salirte como el que te cuento de mi hija, en donde yo tuve que poner consciente. Van a tener que aparecerte mensajitos de advertencia diciendo, cuidado, esta es una acción. ¿Por qué? Porque además de ellos, ya muchos de los casos te hablan empresas muy grandes porque las chiquitas no, pero empresas grandes, ellos ya saben cómo hacerlo, porque caso contrario no podrían vender sus productos en Europa y lo único que hacen es te categoriza. Tienen unos mapas, entonces eso en Ecuador es igual a Europa, todo lo que se añade en Europa hay que aplicar a Ecuador ya.

14. Ya, pero es que ahí me suena este tema de me comenta que hay que ver de dónde vienen las empresas, porque las americanas y las europeas tienen restricciones, pero no así las asiáticas. Pero y ¿la aplicación extraterritorial de la Ley Orgánica no debería ser igual para todas las empresas?.

Claro, pero haz que ocurra entonces como es difícil que hacer que ocurra. Hay que trabajar en que porque las políticas es una forma de autodeclaración. Es una cosa que te obliga a la ley para que tú puedas sancionarte. Si tienes que iniciar procesos. Y el proceso sancionatorio pasará un tiempo, habrá que demostrar, no es automático.

15. ¿Es reactivo?

Ahí es reactivo es en las políticas que es preventivo. ¿Por qué es preventivo? ¿Por qué? Porque son las empresas las que tienen que comenzar a corregir sus políticas y al corregir sus políticas, identificar su brecha y corregir sus actuaciones para ese país en específico. Y ahí es preventivo.

16. Me queda claro. Es por el sistema no y por las protección que en Asia no existe ya. ¿Y una última pregunta, qué podrían hacer las organizaciones de la sociedad civil para promover la Protección de Datos personales de niñas, niñas y adolescentes?

Primero existir. No hay organizaciones de la sociedad civil más que contadas con ni siquiera completo con los dedos de la mano.

17. El centro de autonomía digital. Le hice una entrevista a Ola Bini sobre este tema también. ¿Ya cuál más?

18. Eh bueno, existen ciber derechos de la Andina. Yo no sé qué tan fuerte es.

No se dedica a niñez y adolescencia. Ola Bini tampoco se dedica a la niñez y adolescencia, se dedica a todo. Hay una fundación que se llama *Face*, en Tungurahua hay *Childfund*, que se dedica a temas de niñez y adolescencia y de ahí. Que yo conozca otra, no hay. Ciudadanía y desarrollo puede hablar del tema de usuarios digitales puede hablar del tema, pero no es su foco de atención.

Además, hay que conseguir recursos para eso, no es tan fácil. por eso te digo aquí, el reto en el Ecuador es que existan.

Ya, dónde puedes encontrar estos actores y ver el marco en la política de protección en la, eh y se me fue el nombre en el… En la política pública para una internet sana y segura constructiva que pude hacer gracias a Dios, aunque no era directamente mi competencia, pero a través del Consejo de la igualdad intergeneracional. Francisco Cevallos se llamaba el director que convocó como a 27 organizaciones de públicas y de la sociedad civil para crear esta política que es el único marco que tenemos al día de hoy en el Ecuador y que gracias a Dios le dijimos que iba a tener duración de 10 años porque hasta ahora debería darse seguimiento. Yo acabo de publicar algo. No, no sé si te pueda ser útil, pero te voy a mandar el *link* en el comercio.

Te envío por whatsapp. ¿Dónde te mandé? Ya ay que justo en la columna que escribo para El Comercio publiqué, déjame ver si le menciona la política o solo le mencioné los sitios web, creo que solo les menciona los sitios web porque lo que ves ahí es lo que hay. O sea, es triste, pero es lo único que hay en Ecuador. En otros lados, tú vas a encontrar cosas preciosas aquí agradece que hay esto y eso es porque aquí la presente hizo que pase por mis hijas. Es la ley de Protección de Datos y otro de mis hijos es la política pública de Internet segura.

19. Política pública de Internet segura. Y, esta ¿es del Ministerio de comunicaciones?

No no, no. Es del Consejo Nacional para la igualdad intergeneracional. Solo que yo escribí esa política a puño y letra, sólo que no podía dictarlo porque yo era directorio de una institución que no tiene competencia sobre esto.

Aquí está. Esta es la política pública, está dictada en septiembre de 2020, nos va a regir hasta 2030, si es que nadie decide actualizarla o mejorarla, y es el Consejo Nacional para la igualdad intergeneracional. No sé si lo ves en el en la participación. Estas son las todas las instituciones que participamos y ahí como tú. Puedes ver quienes participaron. Es cierto que ellos también tienen este instituto, ni siquiera es ecuatoriano. Este instituto es no me acuerdo de dónde Child Font y la asociación ecuatoriana, pero la ciberseguridad que no es que tiene como foco niñez y adolescencia. Tiene los pocos ciberseguridad y de ahí está. ¿La dirección nacional de registro de datos públicos, donde yo era directora y la que movió para que esto exista, fui yo, o sea, no es que es iniciativa de mi internos que fue iniciativa del Ministerio de educación, no? Ni siquiera del propio Francisco, que era el director de la de El Consejo Nacional de solo que más bien él me dio espacio, por eso lo logramos.

20. ¿Esta es la única política que hay sobre protección de niños, niñas y adolescentes en internet?

Esto es lo que hay. Esto es lo que hay en el Ecuador y ya te digo y agradece que hay porque me costó sangre, sudor y lágrimas.

21. Muchísimas gracias, Lorena. No tengo más preguntas, no sé si usted quisiera agregar algo. También estaba viendo este proyecto de ley de ciberseguridad. Pero no, no sé qué tanto tiene que ver con el tema usted que conoce más.

Hoy no, tendríamos que demorarnos 1 hora más en el tema es complejito, complejito.

22. Ya. ¿Pero a grandes rasgos y de manera breve, cuál es su opinión? Y también si es que esto tiene que ver con lo que conversamos o no tiene nada que ver.

Tiene que ver en la medida en que ese documento lo que busca es articular a los actores para la lucha del ciberdelito y muchos de los ciberdelitos tienen como principales víctimas niños, niñas y adolescentes. Ahora, que haya una estructura que esté acorde con nuestras líneas y nuestras formas de organización administrativa es cuestionable.

23. justo estaba viendo que hay una doble sanción. Que ahora estas cosas pasan a los militares, a los policías, que existiría una arbitrariedad, sanciones que pueden utilizarse para perseguir políticamente a los enemigos.

O sea, hay una necesidad evidente de coordinación entre las distintas instituciones para una lucha frente contra el crimen y una garantía de la ciberseguridad. Por lo tanto, si se necesita esta ley. Si necesitas coordinaciones, si necesitas que las autoridades puedan luchar contra el cibercrimen, sí. ¿El, cómo es el reto? Y más bien lo que hay que incentivar es que se tiene que seguir dándole importancia a que se necesita y que sí se requiere; y que no hay que decir no a la ley, porque si no va a pasar lo mismo que con la ley de Protección de Datos. Al principio no, no se necesita, no, no. Por eso nos demoramos 13 años en tener. Y es preferible tener una ley. Hay una necesidad se requiere, es una deficiencia, tenemos problemas. En eso sí, hay que trabajar, porque decir no se necesita es falso.

24. Ya muchísimas gracias, Lorena por su tiempo. La verdad es que creo que va a ayudar bastante. ¿Algo más que quisiera agregar? sino para ir cerrando.
Ahí me escribe si tienes alguna cosa y aunque sea te mando un audio ya.

25. Ah no perfecto muchísimas gracias. Yo voy a buscar ahorita mismo esta política pública.

O sea, a mí me ayudas un montón, porque además ya te digo, o sea, si si, yo soy la mamá de la ley de protección de datos, esta fue en mi época y está ya te digo, yo tengo dos hijos y yo hice con conciencia y convicción porque dije algo tengo que hacer porque mis chiquitos necesitan un país en donde al menos se pueda hacer algo.

26. No la no la conocía y obviamente me sirve. Ya. Muchísimas gracias, Lorena que tengas una buena noche.
Gracias igualmente. Chao.

**Santiago Acurio**[493]

1. ¿Cuáles son los principales riesgos para la privacidad y la Protección de Datos personales de los niños, niñas y adolescentes en internet y las redes sociales?

A ver. Comencemos por mencionar que efectivamente los datos personales en este caso de niños, niñas y adolescentes pueden ser considerados como datos sensibles, tomando en consideración que son datos de personas que están en desarrollo entonces estos datos son delicados. Como hay que tener en cuenta el principio del interés superior del niño, estos datos al pertenecer a este grupo etario como son personas en desarrollo, necesariamente son considerados sensibles porque su difusión podría causar en este caso algún problema, alguna estigmatización al desarrollo de estas personas, de este este grupo etario. Entonces por eso es necesario que en el caso de niños y adolescentes se lleve necesariamente una evaluación del riesgo.

Básicamente tomando en cuenta su sensibilidad, estos datos no deben estar publicados libremente en una en una base de datos porque necesitas tener el consentimiento de los de los titulares y como estos titulares son niños y adolescentes, necesitan la autorización de sus padres, en este caso de sus progenitores o representantes legales. En ese sentido, es necesario que se tome en cuenta ese hecho para generar una evaluación de nivelación de impacto de Protección de Datos personales cuando estos datos sean necesarios recogerlos.

2. ¿Existen normativas o políticas que garanticen la Protección de Datos personales y la privacidad de niños, niñas y adolescentes en redes sociales?

O sea, específicamente en redes sociales lo que existe es básicamente tenemos que tomar en cuenta que esto a nivel mundial están aplicando los principios del reglamento europeo de datos personales. Concretamente, por ejemplo, en el caso del Ecuador tenemos el artículo 21 Derecho de niñas, niños, y adolescentes, que dice el derecho básicamente a no ser objeto de decisiones basadas única o parcialmente automatizadas. Entonces no se podrán tratar datos sensibles de niñas, niños, adolescentes a menos que se cuente con la autorización del titular o de su representante legal, cuando dicho tratamiento esté destinado a salvaguardar el interés público esencial, el cual se evalúe en atención a los estándares internacionales de Derechos Humanos y, como mínimo, satisfaga los criterios de legalidad proporcional y necesidad.

---

[493] Licenciado en Ciencias Jurídicas, Abogado y Doctor en Jurisprudencia por la Facultad de Jurisprudencia de la Pontificia Universidad Católica del Ecuador. Especialista Superior en Derecho Penal por la Universidad Andina Simón Bolívar. Magister en Tecnologías para la Gestión y Práctica Docente de la Pontificia Universidad Católica del Ecuador. Magister en Derecho Digital, Transformación Digital y Economía Digital de la UDLA. Dedicado por más de veinte y cuatro años al ejercicio profesional en las aéreas de Derecho Penal, Derecho Procesal Penal, Derecho Informático, dentro de la Fiscalía General del Estado como Director Nacional de Tecnologías de la Información, Jefe de Investigación y Análisis Forense, Jefe Departamental en la Unidad de Flagrancia de Quito, Jefe Departamental en el CEJ de Quitumbe, ex Juez de la Corte Provincial, Sala Única Penal. Capacitador en temas de delitos informáticos e informática forense y docente en varias universidades de la capital. De igual forma coautor del Libro de Derecho y las Nuevas Tecnologías, autor del Libro Derecho Penal Informático, primera y segunda edición, así como autor de varios artículos sobre la temática de derecho informático. Capacitador en cibercrimen de la Organización de Estados Americanos, de la Escuela de la Función Judicial, asistente, participante e instructor en varios cursos y talleres sobre delitos informáticos, cibercrimen, informática forense. Miembro Fundador de la Asociación Ecuatoria de Ciberseguridad AECI, Ex vicepresidente de la Asociación Ecuatoriana de Ciberseguridad AECI, dedicado al ejercicio profesional y la docencia universitaria. Entrevistado el 11 de junio de 2024.

Además, incluye salvaguardar la información para proteger los derechos fundamentales de los interesados. Los adolescentes en ejercicio progresivo de sus derechos a partir de los 15 años, podrán otorgar en calidad de titulares su consentimiento explícito para el tratamiento de sus datos personales siempre que se especifique con claridad sus fines, entonces siempre hay que tener en cuenta que en este caso hay adolescentes mayores de 12 y niños, niñas y adolescentes de 15, así como las niñas, niños para el ejercicio de sus derechos, necesitarán de sus representante legal, los adolescentes mayores de 15 años y niños, niñas y adolescentes de 18 años podrán ejercer en forma directa ante la autoridad de protección de datos personales o ante el responsable del tratamiento. Sus derechos básicamente es lo que nos dice, en este caso el artículo 21 y el artículo 24, inciso segundo sobre el tema del ejercicio de los derechos de Protección de Datos personales.

3. La Ley Orgánica de protección de datos personales entró en vigencia recién en mayo de 2021. Casi tres años después recién se eligió el superintendente. No hay superintendencia. ¿Cómo el Ecuador podría generar contrapeso o garantizar que se cumpla con la protección de datos personales a las grandes empresas de datos como *Facebook*, como *Twitter*? ¿Cómo se logra esto más allá del papel?

O sea, en este caso lo que hay que tener en cuenta es que la propia ley de datos personales te dice básicamente que, vamos a decirlo así, sin perjuicio de las normativas establecidas es del artículo 3 sin permiso de normativa establecida en las instrumentos internacionales ratificados por el estado ecuatoriano que versen sobre esta materia se aplicará la presente ley cuando el tratamientos personales se realiza en cualquier parte del territorio nacional. No obstante, el responsable y el encargado se encuentra domiciliado en cualquier parte del territorio nacional cuando se realiza el tratamiento de datos personales a titulares que reciben el Ecuador por parte del responsable encargado no establecido en el Ecuador.

Entonces, hay que tener en cuenta que si bien es cierto este tema, nos remite a lo establecido en la ley, esta ley está recientemente. O sea, desde el 2021 tenemos la Ley Orgánica de Datos Personales, pero desde la Constitución del 2008 ya tenemos el derecho a la protección de las personales en el artículo 66. Cierto, entonces es ya un derecho humano reconocido, entonces, cómo es un tema de Derechos Humanos es aplicable básicamente en cualquier parte donde se le conozca este derecho humano. Entonces, por eso es que en este caso la superintendencias o todas las agencias creadas para la Protección de Datos personales, al ser el derecho a la protección de las personas de un derecho humano reconocido tanto en la Declaración Universal de Derechos Humanos, debe ser garantizado como tal.

En este caso, que por principio de convencionalidad deben ser aplicables directamente y si tienen mejores derechos que los reconocidos de la Constitución, se aplicarán esos y como digo a nivel internacional, el tema de Derechos Humanos está básicamente muy generalizado, entonces podríamos en este caso demandar o pedir la ayuda internacional para protección justamente de los derechos humanos a nivel de Protección de Datos de datos personales, y aún más si tenemos en cuenta el interés superior del niño en este caso, que también es un principio reconocido por la convención de las Naciones Unidas de los Derechos del Niño, siempre debe prevalecer el interés superior.

En cualquier tratamiento de sus datos personales, las decisiones deben tomarse teniendo en cuenta su bienestar y desarrollo, entonces eso también tiene que tomar en cuenta justamente en las redes sociales, no cierto, Entonces tienen que necesariamente tener un principio de legitimación que es este consentimiento informado. Estamos hablando de *Meta*, que es dueño de *Facebook*, es dueño de *Instagram* que es dueño de *whatsapp*. Entonces podríamos acudir

directamente a las autoridades de Protección de Datos personales en Estados Unidos, en este caso en California, donde se encuentra *Meta*.

Y si por ejemplo, es una persona que está en Ecuador y que se encuentra en Europa se debe hacer eso con entidades de producción de datos personales a nivel europeo, como las que son de cada una de las naciones miembros de la de la Unión Europea. Básicamente recientemente el superintendente de datos personales del Ecuador, que ha sido posesionado, firmó un acuerdo justamente con la Agencia Española de Posición de los personales para pertenecer a la vamos a ir así a la reunión iberoamericana de entes justamente que se dedican a la protección, en este caso de los datos personales.

Entonces este es un paso justamente al tema de Cooperación Internacional. Entonces, depende ya del sistema que se aplique. Entonces si aplicamos el sistema europeo es básicamente el que tenemos nosotros desarrollado en la ley de Protección de Datos Personales. En Estados Unidos tienen el estándar americano y claro en otros países, por ejemplo, los países asiáticos.

La cosa es que ahora ya como autoridad nombrada, tenemos una entidad como la Superintendencia, y aunque falta todo el tema, básicamente administrativo y organizativo ya, pero ya se tiene el Superintendente, que ya ha hecho estos primeros acuerdos que podrían viabilizar una reclamación no es cierto y como digo esto, a nivel de Derechos Humanos podría hacerse sin ningún problema porque es un derecho reconocido en todas las jurisdicciones, por lo menos en las que reconocen la Declaración Universal de los derechos humanos y pertenecen a las Naciones Unidas. Entonces, por ese lado podríamos entrar a hacer ese tipo de cosas.

También a través de la propia Corte Interamericana, porque la Corte Interamericana, la comisión de juristas de la de la Organización Estados Americanos también ha desarrollado una serie de principios, que son aplicables a todos los países miembros de la Organización de Estados Americanos. Entonces por ese lado también podríamos entrar a pedir justamente el cumplimiento de estas obligaciones internacionales en el caso de que sea necesario.

4. ¿En qué se diferencia el sistema americano de protección de datos personales con el europeo?

Tiene el derecho a la privacidad, como digamos, de un sub derecho a los derechos del consumidor, es decir, este es un derecho reactivo, no preventivo y de un derecho de un consumidor de un servicio. Mientras que el sistema europeo es un derecho preventivo.

Entonces lo que ha hecho el Ecuador, porque yo cuando recién empecé a estudiar este tema me venían muchas dudas de este sistema, porque para empezar no existe derecho a la privacidad. En la Constitución existe derecho a la intimidad y de ahí directamente el artículo 66 numeral 19 te habla del derecho a la Protección de Datos. Y me venía mucho esta duda, por ejemplo, se entendería que entraría dentro de este sistema americano porque es reactivo una vez que existen vulneraciones de derechos.

Sobre el Hábeas Data, la misma Corte Constitucional ha señalado en sus sentencias que la que esta garantía constitucional te permite justamente la rectificación, o sea, ejercer todos los derechos de acceso a la información. Eso ya está básicamente en el tema del Hábeas Data, ya que esta en este caso en las normas de la propia Corte Constitucional.

Entonces, la Corte Constitucional reconoce justamente que el Hábeas Data es una herramienta justamente para regular los derechos derivados de la protección de datos personales. De hecho, por eso se habla en la última sentencia de la desnaturalización del recurso de Hábeas Data, ya entonces el Hábeas Data es una garantía jurisdiccional que en este caso puede ser tomada, sea porque se ha violado un derecho o puede ser también para ejercer una medida cautelar.

Entonces lo que te dijo Lorena es verdad. O sea, en el caso americano, pero en este caso, por ejemplo, la legislación de California se aplican los principios del RGPD. Esa es una de las cosas que cambian. Ya entonces ahí sí podemos hacer este sistema básicamente preventivo, pero la Ley Federal en Estados Unidos sigue siendo una ley dice que hay un problema en los servicios prestados o productos entregados básicamente a los consumidores, porque justamente es la comisión de Comercio la que recibe las quejas.

No es un ente de datos personales, sino es una entidad justamente que se dedica al tema comercial, pero en Estados Unidos como es un Estado federal, cada Estado puede poner en este caso sus normas. Entonces algunos, algunos Estados de Estados Unidos han aceptado la propuesta europea.

Entonces hay que saber las diferencias, pero hay que saber dónde está la compañía para ver por qué te vas y cómo le haces para poder en este caso ejercer los derechos, es complicado porque tendríamos que tener, o sea, en el de Europa no hay drama porque tienes un marco regulatorio que es de la Comunidad Europea, que es muy parecido al nuestro. O sea, De hecho es semejante en algunas cosas, ya entonces se puede hacer ese tipo de situaciones.

¿Qué pasa cuando ya claro el tema es cuando no se compatibiliza? En este caso vamos a ir así. O sea, en el caso nuestro, nosotros aplicamos el derecho europeo continental, ya esa es nuestra. Vamos a decir así nuestro sistema jurídico, pero en Estados Unidos muchas veces se aplica lo que se llama el derecho anglosajón, que es un derecho donde generalmente se habla del precedente jurisprudencial, ya que a diferencia de nuestro nosotros tenemos un derecho más positivizado. Entonces es importante saber de dónde es la compañía, que tipo de derecho tienen y cómo lo puedes en este caso ejercer, porque a ver al final del día es cómo generamos tutela sobre un derecho subjetivo, que en este caso es la presión de las personas.

En Ecuador no reconocemos la privacidad, reconocemos la intimidad. el *right to be alone*, que decían los americanos, pero entonces no se ha desarrollado un derecho a la privacidad ya, y de ahí sí a la Protección de Datos personales. Esa es la cosa que hay que tener en cuenta en este tipo de cosas.

5. Ya de aquí también tengo un par de comentarios. Por ejemplo, Ola Bini me dijo que la Ley Orgánica de Protección de Datos personales no tiene enfoque de Derechos Humanos, que tiene un enfoque netamente comercial y que de hecho él y otras organizaciones como APC hicieron antes de que entre en vigencia comentarios. Estas observaciones, sin embargo, no se no se integraron. Como, por ejemplo, que se explique mejor este tema de no ser objeto de tratamiento automatizado. Ninguno de estos enfoques de derechos se integró. Sin embargo, sí se integraron todos los comentarios de las empresas; y otro tema que también va en la misma línea es que el Superintendente no tiene ningún *background* en derechos humanos. Él tiene un *background* netamente en derecho privado. Y vuelvo al tema, o sea, él está elegido, pero no tiene Superintendencia. Así, ¿Cómo hace efectivo la protección de derechos personales si ni siquiera tiene un enfoque de Derechos Humanos?

A ver, el enfoque de Derechos Humanos. A ver, el Enfoque de Derechos Humanos. Nuestra ley tiene que estar alineada a lo que dice la Constitución. ¿O sea, cuál es cuál, qué enfoque de Derechos Humanos piden? Ellos. O sea, básicamente. Que dicen, o sea porque ahí hay que tener en cuenta. Que es un enfoque de Derechos Humanos. ¿Qué entiendes vos por enfoque de Derechos Humanos?

6. Prevenir, investigar, juzgar y, sancionar. Para empezar, tienen una sanción administrativa.

Pero es que es necesario la sanción administrativa. O sea, el tema es saber cuándo tú vas a limitar el derecho de una persona, pues tienes que tener según los parámetros de la corte, la Corte Constitucional y la Corte Interamericana derechos humanos. Tú tienes que tener en este caso que esa limitación del derecho tiene que ser idónea, tiene que ser necesaria y tiene que ser proporcional.

7. ¿La idoneidad, la necesidad y la proporcionalidad se cumple en la Ley Orgánica de Datos Personales? Entre las críticas de Ola, por ejemplo, está crítica, que acabo de recordar, que era que que se sancione a la empresa de acuerdo a sus ingresos. Y, por ejemplo, aquí tengo otra, porque algunas las agregue, obviamente no agregué todas. Con respecto al derecho no ser objeto de una decisión basada únicamente en valoraciones automatizadas, señaló que es importante que se debe especificar que este tipo de decisiones representan la capacidad de decidir por medios tecnológicos y la intervención del ser humano, eso con el propósito de que se aclare las implicaciones que tiene este derecho. Sobre las excepciones del consentimiento para la transferencia, comunicación de datos personales estándares indica que es importante proteger la información que se les recolecte de fuentes de acceso público, porque la recolección masiva de estos datos puede crear perfiles suficientes para vulnerar la privacidad de las personas en su consentimiento. Por lo que se debe eliminar, a excepción de que no es necesario contar el costo de titular para transferencia y comunicación de datos personales.

Es aplicable para realizar los derechos de la privacidad, lo que pasa es que hay que tenerla en cuenta que no hay que ser más papistas que el Papa. El tema es que si tú lees el tema de sansiones personales, si tú lees… Tenemos la ley justamente para llegar a un tema de un mercado digital. Ya, entonces la idea es que tenemos la ley para hacer contrapeso al poder informático que generan básicamente las nuevas tecnologías disruptivas, el *Big Data*, la analítica de datos, la inteligencia artificial, cierto.

Entonces, frente a esas tecnologías disruptivas, tiene que haber ciertos principios básicos como desde el principio de limitación del tratamiento, el principio de minimización, el principio de transparencia. Ya esos son los principios básicos, ya entonces esos principios básicos justamente van a reconocer al ser humano como titular de derechos, entonces no es un objeto de protección, es un titular de derechos ya y en ese sentido se construye el tema de los derechos humanos.

8. ¿Usted considera que la norma nacional es suficiente para garantizar la privacidad de los niños y niñas en las redes sociales?

O sea, es que es un tema integral. Si tú te vas solo a basar en la normativa no te va a ser suficiente, es como lo que decía Schneider, si tú crees que los problemas de seguridad se solucionan con tecnología, vos no sabes ni de la tecnología, ni sabes de la seguridad. ¿Entonces aquí solamente con la norma positivizada, soluciones o garantiza los derechos de los niños y adolescentes? No, es un tema integral, tiene que ser una solución holística, porque solamente, positivamente hablando, no solucionas el tema; es como decir, tenemos ley de transformación digital, pero no existe transformación digital en el Estado.

9. ¿Tampoco hay políticas, o sí?

O sea, eso es parte de la integralidad, tiene que haber una política pública para poder aplicar esto a diferentes niveles de las entidades del Estado. También falta la Superintendencia para que empiece a hacer ese eje conductor y ese eje donde empieza a generar políticas, manuales y reglamentos, porque hay muchas cosas que estando aquí en la ley o estando en el reglamento

todavía no son muy claras. A mucha gente no le parece muy claro, entonces por eso ya viene la autoridad de control que te va a decir "Ah, nos vamos a ir por acá", porque las buenas prácticas nos dicen esto, pero ya tenemos una decisión, ya tenemos una aplicación.

Todavía nos falta resolver, pero en eso estamos, poco a poco, ya poco a poco. Esto es un tema que vamos avanzando, pero tener solo la norma no nos garantiza. Tenemos las leyes del 2021, pero pregunta si es que hay muchas empresas que ya tienen una política de datos personales, si es que tiene hecho básicamente el registro de actividades de tratamiento, si es que ha hecho las evaluaciones de impacto, se ha hecho justamente en este caso el tema de la medición del riesgo. Ya sobre protección de datos personales, entonces hay unas empresas que sí, otras empresas que no, a pesar de que la ley está vigente y pueden caer sanciones administrativas.

10. Sí, pero ahí me viene, por ejemplo, un una idea haciendo analogías. ¿Ejemplo, la minería qué hacen? La empresa de datos tiene una norma que tiene que cumplir, no la cumple, le sancionan. Y es puesto como parte de gastos de producción. Lo mismo pasa con las empresas mineras, hace un estudio de impacto ambiental. Lo hacen mal, lo sancionan, pagan y siguen y siguen dañando la naturaleza y lo ven como que gastos de producción, o sea, el fin último es que se garanticen derechos, no que paguen sanciones y sigan haciendo lo mismo.

Lo que pasa es que hay que tener en cuenta una cosa. La sanción es la primera parte. Es la primera parte, pero mucha gente solo se fija en eso. Lo que puede hacer el superintendente es coger y decirles a las empresas "a ver señores, ustedes han incumplido la ley, muy bien, ya fueron sancionados, les pusimos una multa leve, luego le pusimos una multa grave, entonces la tercera cosa es que ustedes van a dejar de tratar los datos personales." Como decirles a las mineras "señores, ustedes ya no pueden explotar esa minería si ustedes explotan, eso es considerado minería ilegal y ustedes se van presos."

11. ¿Y ahí va mi pregunta, ahí sí se puede suspender el título, el título minero, pero aquí cómo le vas a decir a *Facebook* deja de tratar datos si ya los tienen?

Ya, pero entonces, en este caso lo que pasa es que ahí viene el tema de coordinación internacional. En Estados Unidos y en Europa les han multado a Facebook o a *Meta* por hacer ese tipo de cosas.

Entonces ahí, como ya empezamos a tener estas vinculaciones a nivel de otras organizaciones de Protección de Datos personales, el Ecuador podría recurrir a la Unión Europea y decirles señores, en la Unión Europea han hecho esto, y nos puede servir para aplicar acá.

12. Ya entonces, la respuesta nunca ha sido local y nunca ha sido suficiente, sino que siempre ha sido necesaria una cooperación.

En este caso sí. Tienes que tener Cooperación Internacional, porque vamos a ver, estamos hablando de un efecto global. Entonces, si tienes un efecto así, no puedes generar una sanción local, que no va a llegar a ese efecto global, entonces por eso es que es necesario esa Cooperación Internacional que la ley encontraría no permite con los organismos internacionales. Porque es materia de Derechos Humanos y datos personales, entonces ahí hay que ver si la autoridad nuestra es lo suficientemente ejecutiva como para hacer esto o para llegar a eso.

13. ¿Entonces, usted considera que sería urgente algún convenio internacional sobre Protección de Datos personales?

No ya existe, el convenio es de 108+. Ha sido ratificado por varios países de otros continentes, aquí en Latinoamérica solo firmaron Uruguay y Argentina.

14. ¿Ya, y este tiene un juzgado internacional, una convención, cómo se ejecuta? ¿Cómo garantiza que se cumpla este convenio?

Ese convenio justamente se designa Autoridad Nacional, que sería aquí el superintendente y en este caso tienes la fuerza de la Comunidad Europea.

15. Ya, pero no existe un tribunal internacional.

No, no es que no es para eso no hay tribunales internacionales. Para temas de crímenes de guerra y delitos de lesa humanidad podemos tener tribunales internacionales o al menos que sometas alguna diferencia a un convenio básicamente resolución de un de una, de un arbitraje internacional, pero por lo menos para procesos personales no estaba previsto. No existe un tribunal internacional específico para esto.

16. Ya bueno, continuando con la entrevista. Quería conversar con usted un poco sobre el modelo de negocio de las empresas de datos, que básicamente lo que hacen es extraer datos y comercializarlos, ¿no? Muchas veces sin el consentimiento de sus usuarios. Quisiera saber si usted considera si este modelo de negocio de las empresas de Internet y redes sociales promueve la vulneración de la Protección de Datos personales de niños, niñas y adolescentes.

O sea, básicamente el modelo de negocio tiene que estar necesariamente. Alineado a los estándares, entonces tiene que haber un tratamiento legítimo. El consentimiento es una de las bases legitimadores ya, pero es una de las bases legitimadoras. Puede haber otras bases legitimadoras. Como, por ejemplo, el cumplimiento de una obligación legal, el básicamente hay un orden judicial, puede ser por interés público, puede ser este básicamente por ejecución de medidas precontractuales, por un tema básicamente de intereses vitales, un interés legítimo. Entonces hay que ver la base de legitimación, entonces tiene que haber una base de legitimación ligada al modelo de negocio. Porque si no ese modelo de negocio sería ilegal y estarías cometiendo una infracción. Por lo menos aquí en el Ecuador estás cometiendo. Entonces tienes que tener esa base de legitimación.

17. El problema es que las redes cambian mucho antes que las normas que lo regulan.

Obviamente yo sé que sí, pero en este caso. ¿Como? Esto es una cosa que se aplica básicamente desde que se promulga, si usted en el caso del RGPD, eso está desde el 2018, ya entonces de ahí la normativa europea, por lo menos en redes sociales, que le ha costado a muchas redes sociales. Les ha costado dinero, porque todo ese tipo de cosas han sido multadas en Europa, o sea, han sido multadas. Ahora el tema es claro, esas multas son las que te obligan a cumplir con las normas. Ahora, claro, vamos a decir cómo el Ecuador podría, por ejemplo, sancionar a *Facebook*, sancionar a *Microsoft*, sancionar a cualquier otro proveedor de servicios de redes sociales. Por eso necesitamos del tema de Cooperación Internacional y ahí viene justamente el tema del 108 plus, por lo menos en materia de datos personales.

La autoridad de protección de datos personales en Europa podría sancionar a *Facebook* a *Meta* por un caso que se derivó en el Ecuador, pero siempre y cuando nosotros pertenezcamos o hagamos todo el tema de adecuación a la normativa del 108 plus, que significaría que el Ecuador sea un puesto seguro para que los datos personales sean almacenados aquí en el Ecuador. Entonces ahí viene el tema de que ahí viene a trabajar todo lo que es el tema de seguridad de la información. Necesitamos infraestructura para tener los lugares seguros. Ya de cumplir con las políticas, las buenas prácticas a nivel de infraestructura crítica y eso sí, es un problema que todavía no tenemos, porque para eso se necesita recursos y talento humano.

Ya entonces siempre eso es un problema que no solamente va por el tema de tener la ley o tener los instrumentos legales, sino que también hay que tener otras herramientas como son, en este caso la tecnología, como es en este caso el recurso humano, como es en este caso el recurso financiero para poder invertir y hacer todas las mejoras que se requiere. Ya en Europa tienen 30 años en este tema de Protección de Datos personales y en esos 30 años han avanzado en muchas cosas.

Aquí en el Ecuador, lo que ha tenido un avance significativo son los bancos, las instituciones financieras, ellos sí tienen una buena infraestructura y tienen la tecnología, porque les obliga a las normas internacionales y la propia Superintendencia de bancos, pero no es el único sector en el País, ahí viene ese ese problema que tenemos en el Ecuador, que no tenemos un desarrollo parejo. Entonces tenemos en el sector privado un desarrollo que ha sido impulsado por el propio sector privado, pero en lo público a veces eso no existe.

18. Para buscar soluciones. ¿Qué estrategias pueden implementar los padres para promover una relación saludable y segura con la tecnología, protegiendo así la privacidad de la salud mental de sus hijos?

Tienen que hablar con sus hijos, tienen que hablar con sus hijos. Los padres no pueden hacer nada si no saben. ¿En este caso, por ejemplo, cómo funcionan las redes sociales, qué cosas, qué servicios tienes en las redes sociales? Porque hay que tener en cuenta que a veces los padres pueden ser, en este caso migrantes digitales y los hijos son nativos digitales.

Ya entonces los hijos nacieron con la tecnología, entonces es mucho más fácil que ellos la utilicen, que ellos la puedan, en este caso desarrollar. Es necesario que los padres investiguen. Hay recursos que puedes ver, hay videos en *youtube* que te enseñan, por ejemplo, igual en *tiktok* que tú puedes ver y dan consejos, por ejemplo, de tener programas de antivirus, programas que tenga infowars, programas que básicamente tengas control, un control parental de lo que pueden ver los niños y adolescentes en línea.

Fijar los horarios para el uso de la de la computadora. ¿O el uso del tablet o el teléfono celular? Por ejemplo, yo no le entregaría a una, a un niño ni adolescente un teléfono celular, sino a partir de los 14 años, 15 años, ya yo no le entregaría hasta que no tenga esa edad porque todo ese tiempo le enseñaría a usar o estar consciente de los peligros que se podría exponer en el tema de las redes sociales.

Ya entonces, por eso es necesario que haya esta esta educación inicial en la casa y luego en las aulas, justamente en las aulas. Ya en los en los colegios, en las escuelas, también tener este tipo de concientización, porque la ciberseguridad es la capacidad que tienen las personas, las empresas, las entidades de poder protegerse, de poder protegerse contra incidentes que atentan contra la integridad, la disponibilidad y la confidencialidad de los datos. ¿Cierto? entonces esa capacidad se puede enseñar.

19. ¿Ya y qué podría ser el estado para garantizar el derecho a la Protección de Datos personales de niñas, niñas y adolescentes?

Por ejemplo, ahí sí cumplir con lo que dice la ley, el tema de la educación digital. Ya porque es básicamente un tema prestacional, ya entonces el Estado que promover el uso responsable de las tecnologías de la información y la comunicación, porque también es un derecho garantizado en la Constitución.

El 16.2, en concordancia con el 393 de la Constitución, que es básicamente el tema de la seguridad humana. Ya y parte de la dimensión de la seguridad humana es la seguridad digital, es la ciberseguridad. Entonces, sobre todo, si estamos hablando de una, vamos a ir así de un sector que puede ser vulnerable como son los niños, entonces hay que aplicar ese principio de interés

superior en relación con el principio de acceso a las tecnologías de la información, a la comunicación y el derecho a la seguridad humana que está en la misma Constitución. Entonces, en base a eso, generar política pública, no cierto, para que esto aterrice en las mallas de las escuelas de los colegios y de las propias universidades.

20. Podrían las empresas de tecnología y redes sociales ajustar sus políticas y prácticas para garantizar la Protección de Datos personales y la salud mental de niños, niñas y adolescentes.

O sea, tienen que primero transparentar las cosas. Tener este principio de legitimidad de los datos, entonces, si es que los datos personales alguna vez fueron recogidos sin esta base legitimadora, tendrán que en este caso sus datos borrarse, eliminarse. Y volverse a obtener ya de manera legítima. De manera legítima, no cierto, y entonces hacerle transversal los principios de privacidad por defecto y privacidad por diseño, que son parte de la protección de las personas. Hacer las evaluaciones de impacto, hacer la gestión de los riesgos en Protección de Datos personales y entonces con eso saber si el tratamiento de datos personales en niños y adolescentes fue lícito.

21. ¿Listo doctor, y como última pregunta, qué podrían hacer las organizaciones de la sociedad civil para promover la Protección de Datos personales de niños, niñas y adolescentes en redes sociales e Internet?

Lo que debe hacer la sociedad civil es básicamente estar vigilante por un principio de transparencia. Exigir justamente a los proveedores de servicios, básicamente redes sociales, políticas claras y transparentes sobre la Protección de Datos, o sea que se informe en este caso a la sociedad civil. ¿Qué se hace con los datos personales? ¿Para qué sirve y se tienen en este caso las bases de legitimidad necesarias y que por un principio de limitación y minimización de cuánto tiempo van a utilizar esos datos? No cierto, y que sean los datos mínimos necesarios y que garanticen ese tratamiento legítimo, ya que de ser no ser así, tendrían que eliminarlos.

La ley lo propone tener a disposición de la sociedad civil y los titulares toda la gama de los derechos que da acceso, rectificación, supresión, oposición y, por ejemplo, en este caso el de la portabilidad, el de no ser sujeto a decisiones automatizadas. El tema, justamente de la limitación en el tiempo de los datos, entonces que se pueda posibilitar el ejercicio de sus derechos.

22. Listo doctor. No sé si tiene tal vez algo más que le gustaría mencionar. Algo más que me acabo de acordar. ¿No sé si está usted al tanto del proyecto de ley de ciberseguridad?

Ya fue archivada. O sea, lo que pasa es que no se entendió el proyecto. O sea, sí tenía algunas cosas medias, o sea que no estaba muy claras, pero era un proyecto que era perfectible. Archivarlo es una pérdida para el para el país porque nosotros debemos tener un marco de seguridad digital, un marco de ciberseguridad. Eso se podía corregir. Ya se podía corregir, básicamente aplicando los principios que se encuentran ya en normas internacionales, estándares internacionales como la 27001, como las normas justamente de temas de prevención de riesgos y ese tipo de cosas que sí existen, o sea, es cuestión de darle una afinadita, pero no se entendió bien.

Hay una parte que se desinformo por temas de interés, básicamente privado. No se entendió bien ese tipo de cosas, entonces por eso se archivó, pero es una pérdida. Es que al tema técnico se metió el tema político. Cuando metes el tema político en un tema técnico se jodió.

**Paulina Casares Subía**[494]

1. ¿Cuáles son los principales riesgos para la privacidad y la protección de datos personales de los niños, niñas y adolescentes en Internet y las redes sociales?

La falta de educación y guía para comprender los peligros que se pueden presentar por un usó inadecuado de las redes es muy generalizado el no establecer limites como padres el no guiar y enseñar que la tecnología tienen aspectos positivos pero también negativos es lo que hace vulnerables a estos grupos. Donde se ha perdido la esencia del ejercicio parental y se lo ha traladado a la tecnología (llora le pongo un video, hace berrinche le doy el celular)

2. ¿Existen normativas o políticas que garanticen la protección de datos personales y la privacidad de niños, niñas y adolescentes en redes sociales e Internet?

Existe la Política Pública por una internet segura para niños, niñas y adolescentes de 2020 promovió la creación de la página web www.internetsegura.com actualmente estar al aire nuevamente. Adicionalmente ya contamos con una ley orgánica de protección de datos

3. ¿Considera que el modelo de negocio de las empresas de Internet y redes sociales promueven la vulneración a la protección de datos personales de niños, niñas y adolescentes?

Insisto todo radica en la falta de concienciación hacia el uso de la tecnología y comprender los alcances tanto positivos como negativos que tienen las redes sociales

4. ¿Qué estrategias pueden implementar los padres en el hogar para promover una relación saludable y segura con la tecnología, protegiendo así la privacidad y la salud mental de sus hijos?

La mejor herramienta siempre será la comunicación, guiar a sus hijos, informarse también porque los padres no saben todo pero invitarlos a ver juntos la pagina de internetsegura y hablar siempre la comunicación será la herramienta mas poderosa para guiar a los hijos y sin duda con el ejemplo.

Yo utilizo películas, series en clases con mis alumnos para que puedan evaluar y sacar conclusiones, las debatimos y de eso los mismo chicos van sacando conclusiones y reflexiones muchas veces les sugiero que vean las películas con su familia para que discutan.

5. ¿Qué podría hacer el Estado para garantizar el derecho a la protección de datos personales de niños, niñas y adolescentes?

Ya existen políticas públicas y existen leyes pero la base de todo nace en el núcleo familiar y el refuerzo en el campo de la educación

6. ¿Cómo pueden las empresas de tecnología y redes sociales ajustar sus políticas y prácticas para garantizar la protección de los datos personales y la salud mental de los niños y adolescentes?

Es complejo no se puede controlar lo que pasa al otro ldo del computador muchas redes sociales tienen restricciones de edad sin embargo vemos niños, niñas y adolescentes con autorización de sus padres en ellas.

El control parental es un mecanismo, pero actualmente las generaciones no le dan importancia a la problemas y se lo toma incluso más como un negocio (influencers)

---

[494] Directora de Control y Vigilancia de Mercado en el Ministerio de Producción, Comercio Exterior, Inversiones y Pesca. Información recibida el 24 de mayo de 2024.

7. ¿Qué podrían hacer las organizaciones de la sociedad civil para promover la protección de los datos personales de los niños, niñas y adolescentes en redes sociales e internet?

Capacitar, educar, concientizar y concienciar desde los padres hasta los niños mas pequeños solo educando se puede conseguir resultados

**Patricia**[495]

1. Hoy, 17 de agosto de 2024, nos encontramos aquí con una persona que ha sido usuaria de *Worldcoin*. "Patricia", un gusto.

   Muchas gracias
2. Si me puede decir de donde es y su edad.

   Soy venezolana y tengo 42 años.
3. Muchas gracias, "Patricia". Coméntame por favor su experiencia con *Worldcoin*. ¿Cómo se enteró de él?

Me enteré a través de los mismos compañeros del trabajo y entré, solicité la cita a través de la aplicación y cuando entré, me explicaron muy breve de lo que se trataba, solamente que era como un registro único que iba a poseer más adelante, que se iba a trabajar con criptomonedas, con monedas virtuales, entonces que a futuro iba a servir. Pero yo quería saber más, claro, en ese momento yo me imagino por el corto tiempo que te darán para poder informarte, pero si debieron como decir, ve una bolsa de valores, vamos a trabajar tipo *traiding* y ya eso quería yo saber de qué trataba y por qué.

4. ¿Se enteró porque le dijeron a sus compañeros del trabajo? ¿Qué le dijeron sus compañeros del trabajo?
   Que daban 8 dólares.
5. ¿Qué daban 8 dólares, por qué?

   Por registrarme en esa aplicación.
6. ¿Y cómo le pagaban, en efectivo?

   Uno vende los *tokens*, llaman ellos, los *tokens* los vende uno.
7. ¿Qué es eso?

Ellos, al tú registrarte de inicio te dan como un monto, a mí me dieron en ese momento 8 bitcoins, creo que se llama, 8 *Worldcoins*. Y entonces eso al cambio, al dólar, me dieron, eran como 10 con 19 y el porcentaje que te quitan por pasarlo, 8 con 50. Y por cada referido también te dan una cantidad de *Worldcoins* y tú, si lo deseas, puedes acumularlo y mensual creo que te dan una cantidad, para permanecer activo, te dan una cantidad. Pero en sí, o sea, en vez de decirte "ve, mantengan esto", porque más futuro… tú no sabes qué es más seca, tú te vas a, falta información.

[495] Usuaria de Worldcoin. Entrevistada el 17 de agosto de 2024. Seudónimo para garantizar su anonimato.

8. ¿Se enteró? Se enteró porque le dijeron a sus compañeros, usted fue, se descargó la aplicación, ¿y de ahí?

Cambié, cambié de opinión. De ahí no sé, espero, a ver qué futuro. Ingresé, ajá, te toman los datos, te dan una explicación muy breve que solamente te dicen detallado que es un registro único. Que va a ser como una huella digital, pero a través del iris. Y más nada, pasas como a una cámara y colocas tu retina, más nada, o sea, el ojo.

9. ¿Le dijeron para qué recopilaban su información?

No, que a futuro en vez de utilizar la huella iba a ser el iris. Eso es todo. Y uno ignorante.

10. ¿Le leyeron algún acuerdo, firmó algún contrato?

No, no.

11. ¿Usted sabe para qué van a utilizar su información?

No.

12. Ya, ¿cómo se siente ahora?

Aparte de más ignorante, porque no sé qué va a pasar, o sea, no sé de qué trata, no sé con qué fin. Ahora sí, yo digo, pero quizá la necesidad te hace ciego.

13. ¿Usted conoce a qué podría reclamar este tipo de tratamientos?

No

14. ¿Usted podría obtener efectivo de estas monedas? Digamos, ¿podría transformarlas de *Worldcoins* a dólares, a efectivo?

A través de una persona, de un intermediario. Como casa de cambio, así. Yo le traspaso los *Worldcoins* a ellos y ellos te dan el efectivo a ti.

Listo. Muchas gracias.

**Anexo 5: Análisis del Proyecto de Ley Orgánica de Protección de Datos Personales, realizado por el Centro de Autonomía Digital[496]**

## Proyecto de Ley Orgánica de Protección de Datos Personales

**Centro de Autonomía Digital**

[496] Información recibida el 16 de mayo de 2024.

**Introducción**

El **Centro de Autonomía Digital** (CAD) ha realizado un análisis sobre el **Proyecto de Ley de Protección de Datos Personales**. Para el mismo se utilizó como insumo el Proyecto de Ley enviado a la Asamblea Nacional por parte del ejecutivo, el 19 de Septiembre del 2019.

Adicionalmente se revisaron las cartas enviadas de manera conjunta a la Asamblea Nacional por parte de las organizaciones de la sociedad civil: **APC**, **Derechos Digitales** y **Access Now.**

Los aportes realizados por las organizaciones arriba mencionadas han sido un insumo importante para entender de mejor manera las implicaciones del presente Proyecto de Ley desde un punto de vista legal con un enfoque en los derechos humanos en el mundo digital. Las recomendaciones realizadas son una iniciativa importante para ayudar a crear una ley que sirva para proteger los datos personales de los ciudadanos.

Sobre los comentarios realizados por las organizaciones de la sociedad civil a la carta de las Cámaras de Comercio y Asociaciones afines al ámbito de las telecomunicaciones en lo que se refiere al régimen sancionatorio, creemos importante que se cite como referente el Reglamento Europeo de Protección de Datos, que en su artículo 83 considera sanciones basadas en porcentajes del volumen de ventas anual del año anterior.

**Por otro lado**, el equipo del CAD **realizó un análisis sobre** el Proyecto de Ley **que contempla puntos que no han sido comentados en las cartas elaboradas por APC, Derechos Digitales y Access Now que, consideramos importante examinar.**

## 1. Comentarios de CAD sobre el Proyecto de Ley de Protección de Datos Personales

A continuación presentamos el análisis realizado por el CAD sobre el Proyecto de Ley de Protección de Datos Personales. El documento ha sido estructurado por secciones que agrupan temas específicos de la Ley.

### 1.1. Derechos de Acceso, rectificación, actualización, eliminación, oposición, anulación y/o portabilidad

**Artículo 24. Derecho de Acceso:**

> *El titular tiene derecho a conocer y a obtener del responsable de tratamiento acceso a todos sus datos personales y a la información detallada en el artículo precedente, sin*

*necesidad de presentar justificación alguna.*

*El responsable del tratamiento de datos personales deberá establecer métodos razonables que permitan el ejercicio de este derecho.*

*En caso de que fuera necesario restringir o negar dicho acceso, deberán especificarse las razones concretas de dicha restricción o negativa de acuerdo a lo establecido en la normativa vigente.*

**Análisis del CAD:**

Es importante que los ciudadanos tengan derecho a acceder a la información que es almacenada por los responsables del tratamiento de datos. Sin embargo, esto deviene en el riesgo de que la información personal pueda ser accedida por terceros, de diversas formas entre las que podrían estar:

1. El robo de identidad cuando los protocolos para verificar la identidad de una persona no son los adecuados, haría posible que un tercero logre engañar al responsable del tratamiento de datos para pedir la información de su titular.
2. Si el sistema para acceder a la información personal no está correctamente asegurado, existen vulneraciones mediante las cuales los datos podrían ser robados. Por ejemplo, si la comunicación no se encuentra cifrada y existe un adversario con la capacidad de monitorear el tráfico de la red, este podría aprovechar esta falla para robar la información del titular.

***Ejemplos:***

1. Para el primer caso se podría suponer la situación en la que Juan quiere conocer información personal de José, para esto llama por teléfono a la aseguradora médica de la que José es cliente. Mediante ingeniería social Juan suplanta la identidad de José y logra que la aseguradora le entregue los datos personales de José.
2. Para el caso número dos se puede plantear el siguiente ejemplo: José quiere acceder a la información personal que tiene su aseguradora médica sobre él. Luego de validar correctamente su identidad, la aseguradora envía un enlace a una aplicación donde puede descargarse la información. José accede a su información desde su trabajo, donde la red está siendo monitoreada. El administrador de red del lugar de trabajo de José, podría interceptar la comunicación si esta no se encuentra cifrada (por ejemplo: http) y así acceder a la información de José.

**3.**

***Artículo 26: Derecho de Eliminación:***

*El titular tiene derecho a solicitar la supresión de sus datos personales, a fin de que estos dejen de ser tratados por el responsable del tratamiento de datos personales, cuando:*

1. *El tratamiento no cumpla con los principios de juridicidad, lealtad, transparencia y legitimidad;*
2. *El tratamiento no sea necesario o pertinente para el cumplimiento de la finalidad;*
3. *Los datos personales hayan cumplido con la finalidad para la cual fueron recogidos o tratados;*
4. *Haya vencido el plazo de conservación de los datos personales;*
5. *El tratamiento afecte derechos fundamentales o libertades individuales; o*
6. *Haya revocado o no haya otorgado el consentimiento para uno o varios fines específicos, sin necesidad de que medie justificación alguna.*

*El responsable del tratamiento de datos personales implementará métodos y técnicas orientadas a eliminar, anular, borrar, hacer ilegible, destruir o dejar irreconocibles de forma definitiva y segura, de conformidad con la normativa técnica emitida por la Autoridad de Protección de Datos Personales.*

***Análisis del CAD:***

Este artículo habla acerca del derecho que tienen los titulares para solicitar eliminación de sus datos personales con el fin de que los mismos no sean tratados por el responsable del tratamiento de los mismos.

Estamos de acuerdo con el derecho de eliminación de datos personales. Borrar la información de un usuario de los ambientes de producción no debería ser mayor problema. Sin embargo, es importante considerar que la información también debe ser eliminada de los sistemas de respaldos. Este borrado no siempre es sencillo, ya que pueden existir varias copias distribuidas en distintas localidades físicas. Esto es un problema ya que no se puede garantizar que la información se elimine de todos los respaldos.

A más de los respaldos de datos, se debe eliminar información adicional relacionada con las actividades que realizan los usuarios en la plataforma virtual en cuestión. Esta información es conocida como registros (o *logs* en inglés), y los mismos podrían mostrar los patrones de comportamiento de la persona.

**Ejemplo**:

Al término de un contrato con una operadora móvil, se debería eliminar la información relacionada con el titular, de todas sus bases de datos y respaldos existentes.

La operadora respalda sus bases de datos con la información de todos sus usuarios de manera diaria y mensual. Los respaldos diarios son incrementales y permiten acceder al estado de la base de datos hasta N días atrás. Eliminar la información de una persona de estos respaldos masivos implica un trabajo exhaustivo que, técnicamente, podría no ser viable. De manera similar, eliminar los respaldos mensuales que se almacenan en cintas de datos implica tener que buscar los respaldos en las cintas y eliminarlos de las mismas. Tarea que es todavía más compleja.

1.1. Acceso a Datos Personales por Terceros

Artículo 46. Transferencia o comunicación de datos personales:

*Los datos personales podrán transferirse o comunicarse a terceros cuando se realice para el cumplimiento de fines directamente relacionados con las funciones legítimas del responsable y del destinatario y, además, se cuente con el consentimiento del titular.*

**Análisis del CAD:**

Es importante que se informe de manera clara y específica qué información, a quiénes se la puede compartir y bajo qué circunstancias.

***Ejemplo:***

Juan tiene un emprendimiento y ha contratado un sistema de facturación electrónica en línea provista por la empresa X. La empresa X tiene acceso a todos los datos de las facturas de los clientes de Juan. Entre los datos que se almacenan en las facturas, se incluye: número de teléfono, correo electrónico, cédula de identidad o RUC y nombre completo. Juan nunca informó a sus clientes sobre las prácticas de su proveedor de facturación electrónica con quien comparte sus datos de facturación.

Artículo 47. Acceso a datos personales por parte de terceros:

*[...]*

*El tercero será responsable de las infracciones derivadas de incumplimiento de las condiciones de tratamiento de datos personales establecidas en la presente ley.*

**Análisis del CAD:**

Todos los involucrados en la recolección de datos deben ser responsables sobre el tratamiento de los mismos. El artículo 47 exime de responsabilidad al custodio original de los datos personales. Consideramos que tanto la empresa original como el tercero deben ser igualmente responsables cuando exista algún incumplimiento de la ley.

***Ejemplo:***

Juan tiene un emprendimiento y a ha contratado un sistema de facturación electrónica en línea provista por la empresa X. La empresa X tiene acceso a todos los datos de las facturas de los clientes de Juan. Entre los datos que se almacenan en las facturas, se incluye número de teléfono, correo electrónico, cédula de identidad o RUC y nombre completo.

La empresa X sufre un ataque informático y la información de sus clientes queda expuesta a la Internet. Como está escrito el artículo se entiende que Juan, como dueño de su emprendimiento, no tendría responsabilidad sobre esta vulneración. Consideramos que la responsabilidad debe ser compartida por Juan y la empresa X.

1.1. Vulneración de Datos Personales

Artículo 55: Notificación de vulneración de seguridad:

*[...]*

*La Autoridad de Protección de Datos Personales sólo podrá sancionar al responsable o encargado del tratamiento, cuando la vulneración de seguridad de datos personales ha sido producto de incumplimientos a las medidas de seguridad adecuadas. [...]*

**Análisis del CAD:**

Consideramos que la autoridad de control *siempre* debe sancionar la vulneración de datos personales independientemente de si existió o no un incumplimiento a las medidas de seguridad . Esto debido a que la implementación de medidas seguridad no eliminan la afectación que sufren los titulares por dichas vulneraciones.

***Ejemplo:***

El hospital X archiva electrónicamente imágenes, resultados de pruebas, y el diagnóstico médico de sus pacientes. Este mantiene medidas de seguridad que incluyen la actualización rutinaria del software de equipos y computadoras, la habilitación de cortafuegos y cumple con la norma ISO 27001 relacionada con seguridad informática. Pese a esto el hospital sufre un robo de las historias clínicas electrónicas de sus pacientes. Como está redactado el artículo, el hospital X no podría ser sancionado puesto que cumplió con sus normas de seguridad informática. Consideramos que debería ser sancionado ya que sus pacientes sufrieron una afectación directa por el robo de sus datos clínicos.

Artículo 57: Notificación de vulneración de seguridad al titular:

*[...] No se deberá notificar al titular si se cumple alguna de las siguientes condiciones:*

1. *Cuando el responsable del tratamiento haya adoptado medidas de protección técnicas, organizativas o de cualquier otra índole apropiadas, aplicadas a los datos personales afectados por la vulneración de su seguridad;*

2. *Cuando el responsable del tratamiento haya tomado medidas que garanticen que ya no se concrete el riesgo para los derechos de libertad del titular; y,*

3. *Cuando se requiera un esfuerzo desproporcionado, para lo cual se realizará una comunicación pública, a través de cualquier medio, en la que se informe a los titulares. [...]*

**Análisis del CAD:**

Toda vulneración de seguridad, sin excepción, debe ser notificada a los titulares de los datos. De existir una vulneración, independientemente de las medidas de seguridad tomadas por el responsable del tratamiento de la información, los titulares tienen el derecho a saber que la misma sucedió, así como también, bajo qué circunstancias.

**Ejemplo**:

Un importante "market place" permite comprar en línea a través de tarjetas de crédito. Para efectuar sus ventas, esta empresa cumple con la norma PCI que la habilita a realizar cobros en línea con tarjeta de crédito de forma segura. A pesar de cumplir con los estándares de seguridad informática, el "market place" sufre una filtración de sus datos, que causó el robo de información de tarjetas de crédito de al menos 1000 compradores. El "market place" podría respaldarse en la excepción N.º1 y omitir notificar la vulneración a los afectados justificando el cumpliendo de la norma PCI. Consideramos en este caso, que las personas afectadas deberían ser informadas, pues se vuelven vulnerables a fraudes informáticos debido a que terceros podrían tener acceso a los datos de sus tarjetas de crédito.

Artículo 31: Excepciones a los derechos de rectificación, actualización, eliminación, oposición, anulación y/o portabilidad

*[...]*

*3. Para el cumplimiento de una orden judicial, resolución o mandato motivado de autoridad pública competente;*

*[...]*

**Análisis del CAD:**

Estamos de acuerdo con esta excepción cuando se trata de cumplir con una orden judicial, sin embargo consideramos que "resolución o mandato motivado por autoridad pública competente" es muy amplio. ¿Cualquier autoridad competente podría evitar la rectificación, actualización, eliminación, oposición, anulación y/o portabilidad de datos personales tan solo emitiendo una resolución o mandato?

El sector público debe sujetarse al cumplimiento de este derecho en la ejecución de sus funciones, puesto que este es un actor importante en la recolección masiva de datos personales. Esta excepción podría habilitar a una autoridad pública competente a ser juez y parte.

**Ejemplo**:

La municipalidad X emitió una resolución para utilizar sistemas de reconocimiento facial para identificar a las personas que comentan actos vandálicos en manifestaciones. La resolución contempla el almacenamiento de esta información por al menos un año. Juan es identificado por el sistema durante una manifestación donde ocurrieron actos vandálicos; a pesar de no haber sido parte de esta protesta. Sin embargo, ahora los datos de Juan forman parte de la base de datos de la municipalidad. Con esta excepción Juan no podrá solicitar rectificación, anulación o actualización de sus datos en esta base, puesto que dicha decisión se ejecutó a través de un mandato motivado.

**Artículo 31: Excepciones a los derechos de rectificación, actualización, eliminación, oposición, anulación y/o portabilidad**

*[...]*

*4. Para la formulación, ejercicio o defensa de reclamos o recursos; [...]*

**Análisis del CAD:**

No se encuentra especificado los actores involucrados en esta excepción. Adicionalmente, es importante entender lo que se quiere proteger con la misma.

**Artículo 31: Excepciones a los derechos de rectificación, actualización, eliminación, oposición, anulación y/o portabilidad**

*[...]*

*5. Cuando se pueda causar perjuicios a derechos o afectación a intereses legítimos de terceros;*

*[...]*

**Análisis del CAD:**

Se debería especificar en qué escenarios aplica esta excepción y definir de forma clara: ¿cuándo existe una afectación?, ¿qué se considera intereses legítimos? y ¿qué categorías de terceros serían las afectadas?

***Ejemplo:***

Las operadoras móviles tienen la capacidad de almacenar los datos de geolocalización de sus usuarios y de esta manera monitorear sus patrones de movimiento. Esta información luego es utilizada para recomendar a otras empresas donde abrir un local comercial basada en la cantidad de gente que se moviliza por distintas zonas de las ciudades. Juan considera que su ubicación es un dato sensible y pide a la operadora que borre esta información. La operadora se niega a borrarla porque argumenta que esta información está siendo almacenada con el fin legítimo de promover el emprendimiento en la ciudadanía.

**Artículo 31: Excepciones a los derechos de rectificación, actualización, eliminación, oposición, anulación y/o portabilidad**

*[...]*

*7. Para ejercer el derecho a la libertad de expresión y opinión; [...]*

**Análisis del CAD:**

Este punto amerita mayor discusión, debido a que existen casos donde el derecho a la libertad de expresión entra en conflicto con el derecho a la privacidad.

**Ejemplo**:

Una marcha se transmite a través de un medio de comunicación y uno de los manifestantes muestra un cartel con los datos personales de un tercero que es acusado de haber cometido un delito. No existe un juicio y no se ha comprobado la culpabilidad del individuo cuyos datos han sido expuestos. Tanto el manifestante como el medio de comunicación están ejerciendo su derecho a la libertad de expresión, sin embargo, esto implica que se está vulnerando la privacidad del individuo cuyos datos personales fueron publicados.

**Artículo 31: Excepciones a los derechos de rectificación, actualización, eliminación, oposición, anulación y/o portabilidad**

*[...]*

*9. En los casos en que medie el interés público. [...]*

**Análisis del CAD:**

La ley debe definir el concepto de interés público, ya que es un término jurídico indeterminado que actualmente no está definido en ninguna normativa ecuatoriana. Esto hace que pueda prestarse a múltiples interpretaciones.

***Ejemplo:***

Juan es un reconocido deportista que se ha visto envuelto en presuntas acusaciones de infidelidad, expuestos por los medios de comunicación a la opinión pública. La condición de Juan como figura mediática es usada como justificación para que su caso sea de interés público. Esto tiene una repercusión directa en la vida profesional y privada de Juan, quien no podría oponerse a la divulgación de su información personal debido a esta excepción.

**Artículo 31: Excepciones a los derechos de rectificación,**
***actualización, eliminación, oposición, anulación y/o portabilidad***

*[...]*

*10. En el tratamiento de datos personales que sean necesarios para el archivo de información que constituya patrimonio del Estado, investigación científica, histórica o estadística.*

*[...]*

**Análisis del CAD:**

Es necesario se especifique qué actores entran en esta excepción y el alcance de lo que se refiere

con investigación científica, histórica o estadística.

***Ejemplo:***

El gobierno central inició un proyecto de investigación científica basado en información publicada por la ciudadanía en redes sociales. Argumentan que el objetivo de la misma es analizar los patrones de comportamiento de la gente y así brindar mejores servicios. Juan es un activista en contra de la minería a cielo abierto y considera que la información recolectada es sensible puesto que puede poner en riesgo su trabajo por lo que no quiere formar parte de esta investigación. La solicitud de Juan puede ser rechazada debido a esta excepción.

**Artículo 33. Derecho a no ser objeto de una decisión basada únicamente en valoraciones automatizadas**

> *El titular tiene derecho a no ser sometido a una decisión basada únicamente en valoraciones que sean producto de procesos automatizados, incluida la elaboración de perfiles, que produzcan efectos jurídicos en él o que atenten contra sus derechos y libertades fundamentales [...]*

**Análisis del CAD:**

Es importante que se especifique que las decisiones basadas únicamente en valoraciones automatizadas representa la capacidad de decidir por medios tecnológicos sin la intervención del ser humano. Se debe enfatizar también que las decisiones automatizadas pueden basarse en cualquier tipo de datos, el propósito de esta recomendación es que se aclare las implicaciones que tiene este derecho.

**Artículo 33. Derecho a no ser objeto de una decisión basada únicamente en valoraciones automatizadas**

> *[...]*
>
> *1. Solicitar una explicación motivada sobre la decisión tomada por el responsable o encargado del tratamiento de datos personales;*
>
> *[...]*

**Análisis del CAD:**

La ley debe obligar al responsable o encargado de datos a responder con una explicación sobre decisiones tomadas de forma automatizada al interesado/a en un bien o servicio en particular. Es importante que se justifique de manera clara cómo se realiza el tratamiento de los datos en la toma de dichas decisiones, ya que las mismas pueden vulnerar otros derechos como el acceso a servicios, restricciones de créditos, entre otros.

**Ejemplo**:

Juan solicita un crédito hipotecario a través del portal web del banco público BIESS. Se le pide que introduzca sus datos y el algoritmo del banco le dice si se le concederá el préstamo o no y le sugiere un tipo de interés. Consideramos que el BIESS debe informar a Juan la lógica que sustenta el tratamiento de los datos y que desemboca en la decisión de "sí" o "no". Con la actual redacción del artículo, se entiende que el BIESS puede recibir la solicitud, pero no está obligado a justificar la razón de la misma.

**Artículo 33. Derecho a no ser objeto de una decisión basada únicamente en valoraciones automatizadas**

*[...]*

*No se aplicará este derecho cuando:*

*1. La decisión es necesaria para la celebración o ejecución de un contrato entre el titular y el responsable o encargado del tratamiento de datos personales;*

*[...]*

**Análisis del CAD:**

Esta excepción abre la posibilidad de restringir otros derechos fundamentales basado en la firma de un contrato, por ejemplo, los términos de uso de las aplicaciones web pueden ser considerados como un contrato, los mismos que suelen ser extensos y muchas veces la gente no los lee. Si los términos no son claros, con esta excepción, se estaría limitando el derecho a no ser objeto de una decisión basada únicamente en valoraciones automatizadas.

***Ejemplo:***

Al momento de crear una cuenta en redes sociales se debe aceptar los términos de uso. Es común que la necesidad de usar estas plataformas y la gran extensión de los términos de uso, hagan a los usuarios aceptar dichos términos de manera poco informada. Existe la posibilidad que dentro de estas condiciones, el usuario acepte recibir publicidad direccionada basada en decisiones automatizadas ejecutadas por la plataforma. Al ser confusos los términos de uso, el usuario podría ceder sus derechos inconscientemente al aceptarlos.

**Artículo 33. Derecho a no ser objeto de una decisión basada únicamente en valoraciones automatizadas:**

*[...]*

*No se aplicará este derecho cuando:*

*[...]*

*2. Está autorizada por la normativa aplicable, orden judicial, resolución o mandato motivado de autoridad pública competente, para lo cual se deberá establecer medidas adecuadas para salvaguardar los derechos fundamentales y libertades del titular; [...]*

**Análisis del CAD:**

Es necesario que se defina el alcance del término "normativa aplicable". Adicionalmente, permitir a la autoridad pública competente autorizar la toma de decisiones basadas únicamente en valoraciones automatizadas, entrega demasiado poder a una persona y/o entidad que también debe estar sujeta a la ley.

***Ejemplo:***

Un Gobierno Autónomo Descentralizado (GAD) puede ser considerado una autoridad pública competente. El GAD implementa un sistema de reconocimiento facial, que de manera automatizada, identifica cuando un sospechoso circula por las calles de la ciudad y notifica a la policía para su detención. Este tipo de sistemas han demostrado no ser 100% fiables y han existido casos en los que se ha detenido personas por falsos positivos, violando así el derecho a la presunción de inocencia.

Como está escrito el artículo, cualquier autoridad pública competente podría implementar sistemas que no respeten el derecho de las personas a no ser objeto de decisiones basadas únicamente en valoraciones automatizadas.

**Artículo 48: Excepciones de consentimiento para la transferencia o comunicación de datos personales**

> *No es necesario contar con el consentimiento del titular para la transferencia o comunicación de datos personales, en los siguientes supuestos:*
>
> *1. Cuando los datos han sido recogidos de fuentes accesibles al público; [...]*

**Análisis del CAD:**

Es importante proteger la información que se recolecta de fuentes de acceso público, porque la recolección masiva de estos datos puede crear perfiles suficientes para vulnerar la privacidad de las personas sin su consentimiento. Con esta excepción la ley habilita que un tercero maneje a su conveniencia los datos de las personas sin ningún tipo de control y sin infringir la presente ley. Es importante considerar que la información accesible a través de fuentes abiertas incluye las publicaciones en redes sociales, información de sistemas estatales, publicaciones de prensa, entre otras.

***Ejemplo:***

Juan, un periodista de investigación, escribe un artículo que revela casos de corrupción del gobierno de turno. La agencia de inteligencia ha recolectado información de Juan a través de fuentes abiertas que incluye pago de impuestos, propiedades, publicaciones en redes sociales, entre otras. El perfil de Juan podría ser una herramienta para persuadirlo de no seguir publicando en contra del gobierno sin que esto implique haber infringido la ley.

**Artículo 48: Excepciones de consentimiento para la transferencia o comunicación de datos personales**

*No es necesario contar con el consentimiento del titular para la transferencia o comunicación de datos personales, en los siguientes supuestos:*

*[...]*

*5. Cuando la comunicación de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre salud [...]*

**Análisis del CAD:**

Esta excepción debe contemplar que quienes almacenan los datos para los fines expuestos deben ser responsables de manejar los mismos de manera segura y no los pueden usar para otros fines diferentes a los especificados para su actividad inicial.

***Ejemplo:***

Dentro de la crisis sanitaria generada por el COVID-19 se han desarrollado múltiples herramientas que buscan brindar ayuda para la prevención del virus. En Guatemala, el gobierno promovió el uso de la aplicación móvil "Alerta Guate", que tiene como finalidad informar acerca de las acciones preventivas a la comunidad. Sin embargo, un estudio realizado por Global Witness reveló que la aplicación proveía de datos de geolocalización de sus usuarios al proveedor de la app, que ha hecho uso de los mismos para fines comerciales, sin previo consentimiento.

Si bien es cierto que la aplicación nació con la finalidad de colaborar en los esfuerzos de contención y prevención en la crisis sanitaria, su utilización violenta la privacidad de sus usuarios bajo el amparo de esta excepción.

**Artículo 69: Casos excepcionales de transferencias o comunicaciones internacionales**

*En aquellos casos donde no se cumpla con los criterios de niveles adecuados de protección o de garantías adecuadas de protección, la Autoridad de Protección de Datos Personales podrá autorizar transferencias o comunicaciones internacionales de datos personales, en los siguientes casos:*

*1. A países u organismos internacionales que brinden garantías adecuadas para la protección de datos personales sin que necesariamente exista una ley específica o Autoridad de Protección de Datos Personales, para lo cual será necesaria la suscripción*

*de un convenio o tratado internacional; [...]*

**Análisis del CAD:**

Se debe tener cuidado con esta excepción, ya que los convenios y tratados internacionales se superponen en jerarquía a las normas dictadas en la legislación ecuatoriana. De esta manera se podría vulnerar los derechos consagrados a los ciudadanos en la presente Ley.

***Ejemplo:***

Un grupo de activistas ambientales se oponen a la explotación minera de una empresa multinacional, la misma que solicita ayuda al gobierno de su país para solventar el problema. Este gobierno decide celebrar un convenio con el Ecuador que permita realizar la actividad extractivista, además de recolectar y transferir información del grupo ecologista al país de origen de la multinacional. El convenio habilita a la empresa minera a transferir datos personales del grupo activista, sin su consentimiento al país de origen de la empresa minera.

**Artículo 69: Casos excepcionales de transferencias o comunicaciones internacionales**

*En aquellos casos donde no se cumpla con los criterios de niveles adecuados de protección o de garantías adecuadas de protección, la Autoridad de Protección de Datos Personales podrá autorizar transferencias o comunicaciones internacionales de datos personales, en los siguientes casos:*

*[...]*
*4. Cuando la transferencia internacional tenga comofinalidad el cumplimiento de una obligación legal oregulatoria; [...]*

**Análisis del CAD:**

Esta excepción no debería existir por ser muy amplia. En caso de conservarla, se debería detallar de manera más específica su alcance.

**Artículo 69: Casos excepcionales de transferencias o comunicaciones internacionales**

*En aquellos casos donde no se cumpla con los criterios de niveles adecuados de protección o de garantías adecuadas de protección, la Autoridad de Protección de Datos Personales podrá autorizar transferencias o comunicaciones internacionales de datos personales, en los siguientes casos:*

*[...]*

*7. Cuando la transferencia sea necesaria por razones de interés público; [...]*

***Análisis del CAD:***

La ley debe definir el concepto de *interés público*, ya que es un concepto jurídico amplio que actualmente no está definido en ninguna normativa en el Ecuador. Esto hace que se pueda prestar a múltiples interpretaciones que vulneren otros derechos.

## CAPÍTULO XI AUTORIDAD DE PROTECCIÓN DE DATOS PERSONALES

Este capítulo habla sobre las competencias de la Autoridad de Protección de Datos Personales. No se copia este artículo de manera íntegra por su extensión, pero puede ser revisado en el Proyecto de Ley.

**Análisis del CAD:**

La Autoridad de Protección de Datos debe garantizar la aplicación de las mejores prácticas en seguridad informática, que ayuden a mitigar los riesgos a la privacidad e integridad de los datos derivados del avance acelerado de las tecnologías de la información. Esto implica disponer del talento humano con el conocimiento necesario para trabajar en la implementación de las mismas.

Sabiendo que actualmente el Ecuador no cuenta con un grupo considerable de profesionales especialistas requeridos para avalar las decisiones técnicas emitidas por la Autoridad de Protección de datos en uso de sus facultades, esta es una limitante considerable a la hora de respaldar las decisiones técnicas tomadas por el ente de control, que debería ser considerada en el Proyecto de Ley al momento de su constitución.

1.1. Otros

**Artículo 5: Términos y Definiciones**

El Artículo 5 define términos que son utilizados a lo largo de la Ley. No se copia este artículo de manera íntegra por su extensión, pero puede ser revisado en el Proyecto de Ley.

**Análisis del CAD:**

Existen términos dentro del Proyecto de Ley que consideramos deben ser definidos o se debe mejorar su definición:

- *Metadato:* Es importante definir qué son los metadatos y la relación de los mismos con los datos personales. Un metadato por si solo no va a desanonimizar a una persona, sin embargo la combinación de varios metadatos, sí.
- *Interés público:* Este término se utiliza varias veces en el proyecto de ley, consideramos que puede prestarse a varias interpretaciones por lo que debería definirse de forma específica y asimismo, precisar su alcance.
- *Valoración automatizada: Es importante que se defina explícitamente lo que implica una valoración automatizada.*

**Capítulo IV CATEGORÍAS ESPECIALES DE DATOS PERSONALES**

En el Capítulo IV se definen las categorías especiales de datos personales y contempla los artículos 38 al 45. No se copian los artículos de manera íntegra por su extensión, pero pueden ser revisados en el Proyecto de Ley.

**Análisis del CAD:**

Los *datos de autenticación* deben estar incluidos en las categorías especiales de datos personales porque contemplan al menos el nombre de usuario, contraseña y certificados digitales. Estos datos son particularmente importantes porque permiten acceder a sistemas que contienen información personal. Si los mismos no son correctamente resguardados, pueden sufrir vulneraciones por parte de terceros que podrían acceder a sistemas donde se guarda la información del titular.

**Acciones Concretas**

1. Identificar y vincular a organizaciones locales y equipos multidisciplinarios que puedan actuar

   como aliados para trabajar de manera conjunta en estrategias que busquen mejorar el Proyecto de Ley.

2. Escribir una carta dirigida a la Asamblea Nacional de manera conjunta con los actores que se

   haya logrado vincular y solicitar audiencia a fin de exponer todos los comentarios y/o inquietudes sobre el presente Proyecto de Ley.

3. Generar espacios de discusión abiertos en torno al presente Proyecto de Ley tales como: conversatorios en universidades, eventos virtuales, mesas de debate, entre otros.