

AUDIENCIA TEMÁTICA CIDH:

2026

***RENDICIÓN DE CUENTAS DE LAS PLATAFORMAS
DIGITALES Y SU IMPACTO EN LOS
DERECHOS HUMANOS***



RESUMEN EJECUTIVO

Desde el Centro de Estudios de Derecho, Justicia y Sociedad - DEJUSTICIA, Colombia; RedPaPaz, Colombia; Artigo 19 Brasil e América do Sul, Brasil; CELS, Argentina; Conectas Direitos Humanos, Brasil; Instituto Alana, Brasil y Tech Justice Law, United States of America, solicitamos a la Comisión Interamericana de Derechos Humanos (CIDH) la realización de una audiencia temática sobre “Rendición de cuentas de las plataformas digitales y su impacto en los derechos humanos”. Nuestra solicitud fue aprobada y la audiencia se llevó a cabo en Washington DC el 4 de agosto de 2026, en el marco del periodo de sesiones 197 de la CIDH.

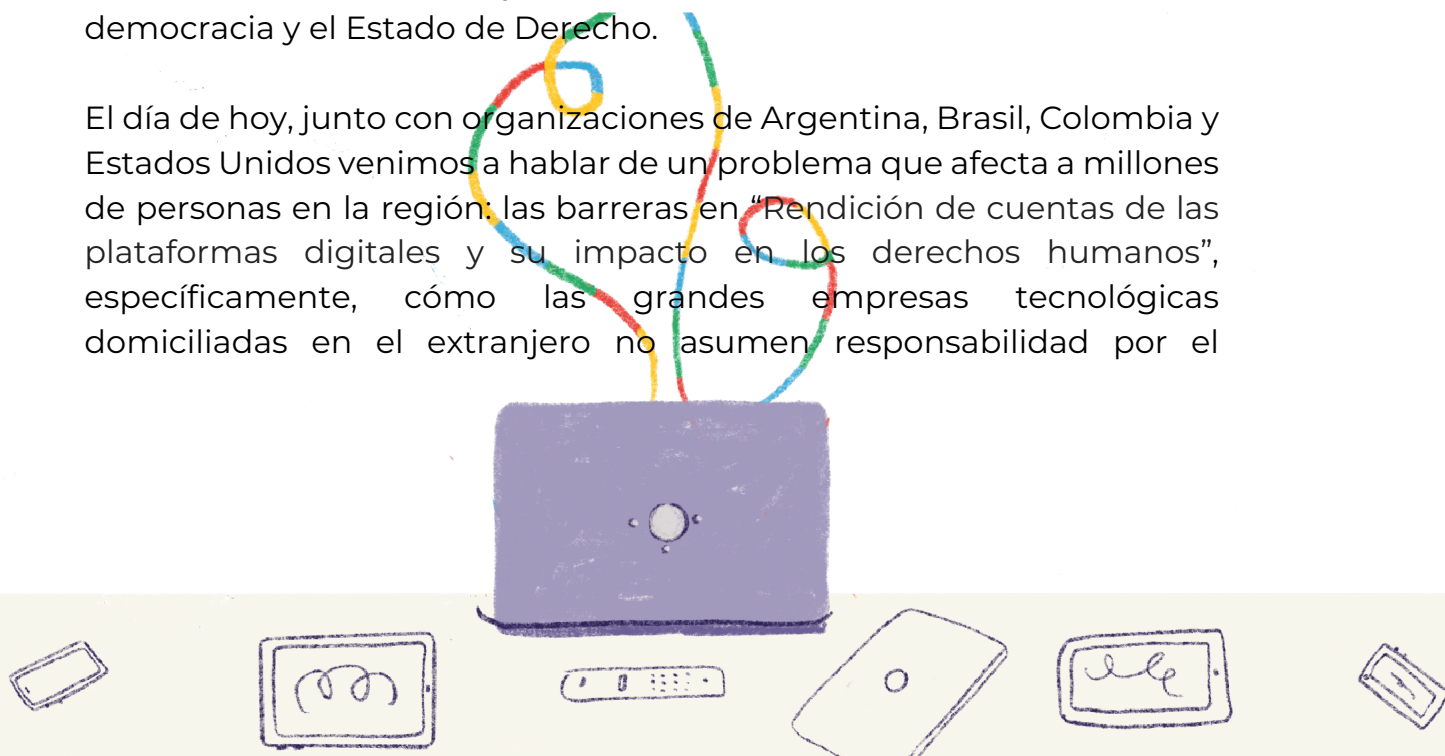
Como parte del proceso de preparación para la audiencia, las solicitantes presentamos unos insumos previos a la CIDH, que hemos decidido hacer públicos por su utilidad académica. Asimismo, como parte del resumen ejecutivo de esta publicación, presentamos las intervenciones orales de cada uno de los representantes de las organizaciones solicitantes.

APERTURA: DEJUSTICIA

Honorables miembros de la Comisión Interamericana de Derechos Humanos, y relatores, gracias por este valioso espacio que da cuenta de la gran relevancia del tema para la región.

Mi nombre es Maryluz Barragán González y soy subdirectora del Centro de Derecho, Justicia y Sociedad – Dejusticia. Una ONG colombiana con más de 20 años de trabajo de defensa de los derechos humanos, la democracia y el Estado de Derecho.

El día de hoy, junto con organizaciones de Argentina, Brasil, Colombia y Estados Unidos venimos a hablar de un problema que afecta a millones de personas en la región: las barreras en “Rendición de cuentas de las plataformas digitales y su impacto en los derechos humanos”, específicamente, cómo las grandes empresas tecnológicas domiciliadas en el extranjero no asumen responsabilidad por el



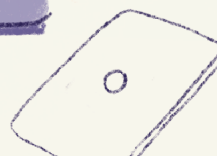
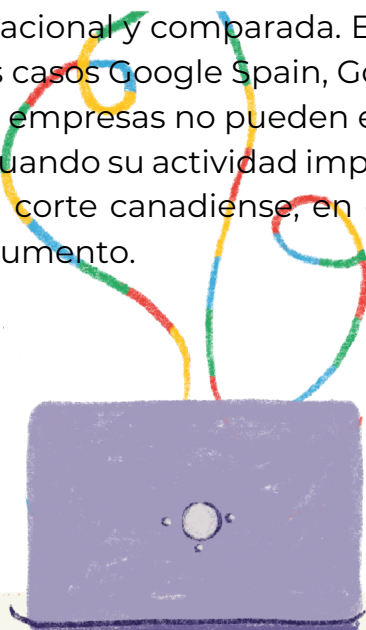
tratamiento de datos personales de los nacionales, y con ello, violan masivamente nuestros derechos al habeas data y otros derechos fundamentales.

En esta primera parte me enfocaré en la problemática de la jurisdicción y las leyes aplicables a las empresas tecnológicas. Luego mis colegas desarrollarán las afectaciones concretas en asuntos como la integridad democrática, la salud mental y los efectos diferenciados en las infancias.

Las empresas tecnológicas basan su modelo de negocio en la explotación masiva de datos personales. A través de tecnologías como las cookies, SDKs (software development kits) y píxeles (que se instalan en los dispositivos de los usuarios) recolectan, almacenan y monetizan información íntima: ubicación, hábitos de consumo, e incluso datos de salud. Sobre esto último existen investigaciones de 2022 que encontraron que rastreadores de Meta en sitios web de telesalud enviaban a Facebook información íntima de los pacientes. Todo en el marco de la legalidad, lo que da cuenta de una brecha regulatoria.

Lo importante para esta Comisión es esto: ese tratamiento de datos ocurre físicamente en nuestros países, en los países de América Latina. El dispositivo donde se instala la cookie, donde corre el SDK, donde se despliega el píxel, está en Colombia o en cualquier otro país de la región. No es un tecnicismo: es donde ocurre el daño.

Sin embargo, empresas como Google han iniciado acciones judiciales en Colombia para desconocer la competencia de la Superintendencia de Industria y Comercio, argumentando que el tratamiento ocurre en servidores extranjeros. Esta postura contradice la tendencia jurisprudencial internacional y comparada. El Tribunal de Justicia de la Unión Europea, en los casos Google Spain, Google v. CNIL y Schrems I y II, ha sido enfático: las empresas no pueden evadir la ley local alegando domicilio extranjero cuando su actividad impacta a personas dentro del territorio. Incluso una corte canadiense, en el caso Giustra vs. Twitter, rechazó el mismo argumento.



Es decir: el mundo se mueve hacia el reconocimiento de la jurisdicción local. Pero los países del Sur Global, sin el peso político de la Unión Europea, enfrentan mayor resistencia de estas empresas para hacer valer sus propias leyes. De hecho, Estados Unidos, de manera más reciente, ha firmado acuerdos comerciales recíprocos con cuatro países de América (Argentina, Ecuador, Guatemala y El Salvador) que podrían debilitar la protección de los datos personales. Mi colega del CELS lo explicará con más detalle.

Esto no es un debate abstracto. Cuando estas empresas evaden la jurisdicción, dejan indefensas a millones de personas frente al uso manipulador de sus datos. Aquí hablamos de afectaciones concretas a la salud mental por diseños adictivos, riesgos para grupos vulnerables, e incidencia indebida en procesos democráticos, como lo veremos en las próximas intervenciones.

Por eso, solicitamos respetuosamente a la Comisión que considere: Primero, la elaboración de un informe temático o lineamientos regionales sobre la responsabilidad de las empresas tecnológicas frente a los derechos humanos, incluyendo el habeas data, en la región. Segundo, que inste a los Estados miembros a fortalecer sus marcos normativos de protección de datos con criterios claros de jurisdicción, en línea con los estándares que ya existen en el derecho comparado.

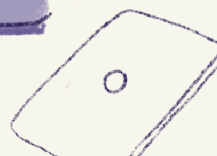
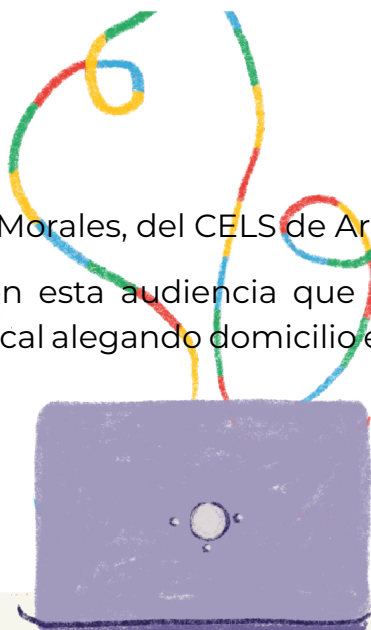
La pregunta de fondo es simple: ¿pueden las empresas más poderosas del mundo decidir a qué leyes se someten? Nuestra posición es que no. La protección de derechos humanos no puede depender de la ubicación de un servidor.

Muchas gracias.

CELS

Mi nombre es Diego Morales, del CELS de Argentina.

Ya se ha señalado en esta audiencia que "las empresas no pueden eludir la legislación local alegando domicilio en el extranjero cuando sus



3



actividades afectan a personas dentro del territorio". Agregamos ahora una preocupación más, que es la cuestión de la transferencia transnacional de los datos personales.

A la tendencia de debilitamiento de los marcos de rendición de cuentas de las plataformas se suma el riesgo vinculado a los acuerdos económicos bilaterales promovidos por los Estados Unidos que modifican estándares de protección de datos de otros países, para facilitar el tráfico transnacional de datos hacia aquel país. En particular, nos vamos a referir al acuerdo que en febrero de este año firmaron Estados Unidos y Argentina.

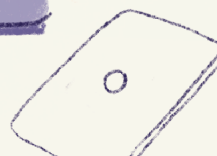
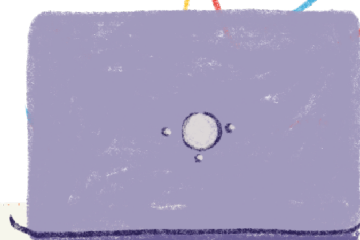
Se trata de un acuerdo aún no ratificado sobre "inversión y comercio recíproco" que implica que la Argentina reduce o elimina barreras arancelarias y no arancelarias y otorga privilegios comerciales a los productos estadounidenses.

Este acuerdo ya fue citado en la audiencia de ayer sobre la situación del derecho a la salud en Argentina, porque nuestro país por decisión unilateral decidió derogar los criterios estrictos de patentabilidad de medicamentos.

En lo que aquí interesa, el artículo 2 del anexo 3 del acuerdo contiene una modificación del marco jurídico nacional en materia de datos personales. Y establece que, a efectos de la transferencia de datos a los Estados Unidos, Argentina considerará que los Estados Unidos garantizan una protección jurídica "adecuada" para dichos datos. Argentina, además, "proporcionará certeza respecto a la posibilidad de transferir datos personales desde su territorio a los Estados Unidos".

Sin embargo, el artículo 12 de la Ley de datos personales prohíbe la transferencia de estos datos de cualquier tipo a "países u organizaciones internacionales o supranacionales que no ofrezcan niveles adecuados de protección".

La agencia en materia de Acceso a la Información Pública, que es la autoridad que determina qué países y organizaciones ofrecen una protección jurídica adecuada, nunca consideró a los Estados Unidos en la lista de países que ofrecen protección jurídica de esas características. A juicio de esta Agencia:



- Estados Unidos carece de una normativa federal uniforme sobre el tratamiento de datos personales y de una autoridad de control eficaz.
- Y que las normas de “autorregulación” no son exigibles ni uniformes en los cincuenta estados de la Unión.

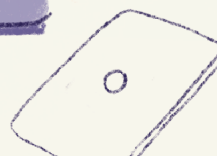
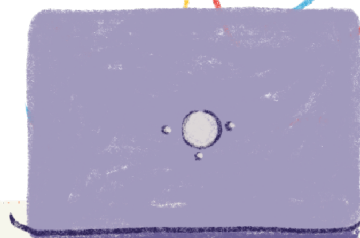
El acuerdo entonces crea una excepción a la prohibición de las transferencias de datos personales. Esto puede darse, por la entrada en vigencia de un “tratado internacional del que Argentina es parte”, cuestión que habilita la propia ley de datos personales, o porque la Agencia de Acceso a la Información Pública emita una resolución en la que se declare que Estados Unidos es una jurisdicción adecuada. Ello en contra de la evaluación que ya ha formulado en distintas ocasiones la agencia Argentina.

Cualquiera de estas situaciones implicaría autorizar transferencias internacionales de datos a un país que no es considerado una “jurisdicción adecuada” por el Gobierno argentino sin que las circunstancias en dicho país hayan cambiado. O más grave aún, que hayan empeorado por el uso de los datos como herramienta de vigilancia (por ejemplo, contra migrantes) y/o por su alianza estratégica con empresas de inteligencia artificial y procesamiento de grandes masas de datos.

Con este tipo de acuerdos, la transferencia o venta de datos personales a responsables o encargados del tratamiento estadounidenses (incluidas las grandes empresas tecnológicas) ya no estará sujeta a la normativa de la ley de protección de datos personales de Argentina.

La Corte Suprema en un reciente caso declaró inconstitucional un artículo de la ley de datos personales que permitía la cesión de datos personales entre agencias del mismo Estado, pero sin el consentimiento específico de los interesados. El Tribunal sostuvo que los artículos 19 (autonomía) y 43, apartado 3 (habeas data), de la Constitución Nacional consagran el derecho a la autodeterminación informativa —cuestión ya reconocida por la Corte Interamericana de Derechos Humanos en el caso CAJAR—.

Con todo, las transferencias de datos a Estados Unidos (sea a las autoridades o a las empresas) dejarán de estar sujetas a las garantías



constitucionales o los principios establecidos por la Ley de Protección de Datos Personales, como el consentimiento, finalidad o la habilitación de una instancia de protección legal de habeas data para limitar su tratamiento. Tampoco estas transferencias, en los términos del acuerdo, estarán alcanzadas por las facultades de supervisión de la Agencia de Acceso a la Información Pública.

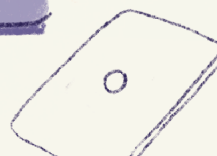
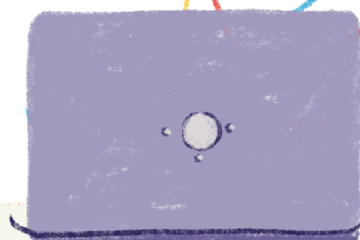
En consecuencia, proponemos a la Comisión que incluya en el Informe mencionado un análisis particular sobre los efectos de los acuerdos transnacionales como el señalado, en los marcos nacionales de protección de datos, y analice su compatibilidad con los compromisos asumidos en el marco de la CADH.

ARTIGO 19

Estimados representantes de la Comisión Interamericana de Derechos Humanos, buenos días. Mi nombre es Raquel da Cruz Lima y represento a ARTÍCULO 19 Brasil y América del Sur.

El propósito de esta intervención es llamar la atención de la Comisión sobre uno de los aspectos estructurales que permiten a las grandes plataformas digitales manipular el debate público y afectar la integridad democrática y el ejercicio de los derechos humanos en las Américas: la profunda concentración del poder económico.

Como ya han expuesto mis colegas, el modelo de negocio de estas corporaciones se basa en la recolección masiva de datos personales y en la amplificación algorítmica para la retención de la atención. Este modelo no solo genera ganancias extraordinarias, sino que además es un mecanismo que produce y reproduce la concentración del poder económico. Al controlar los datos de miles de millones de personas y las infraestructuras a través de las cuales circula la información, estas empresas acumulan un poder suficiente para definir las condiciones bajo las cuales pueden circular las ideas y los pensamientos. Las implicancias son directas para la libertad de pensamiento y de expresión, para los derechos políticos, la igualdad y la no discriminación, tal como se definen en los artículos 13, 23, 24 y 1.1 de la CADH. El funcionamiento de los sistemas de recomendación basados en el



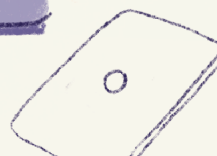
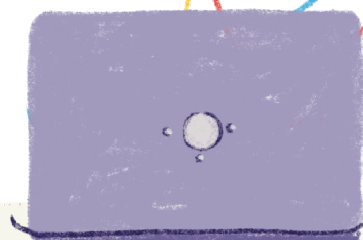
engagement prioriza la circulación de contenidos extremos y polarizantes, afectando de manera desproporcionada a los grupos históricamente marginados y obstaculizando su participación política en condiciones de igualdad. Otra dinámica que afecta la participación política de los grupos históricamente vulnerables, en especial la comunidad LGBTQIAPN+, es el "shadow banning", es decir, la reducción de la visibilidad o del alcance de sus contenidos.

Este poder de las plataformas para definir qué voces serán escuchadas en la esfera pública deriva de la concentración de poder en manos de unas pocas empresas. De hecho, en el informe "Inclusión Digital y Gobernanza de Contenidos", la RELE y la Comisión afirmaron que Internet está marcada por el dominio de unos pocos grandes actores del sector tecnológico, lo que afecta negativamente la diversidad en la infraestructura de la comunicación. Quisiera también señalar que el Marco Jurídico Interamericano sobre el Derecho a la Libertad de Expresión reconoce que los monopolios u oligopolios en la propiedad y el control de los medios de comunicación restringen la pluralidad y la diversidad de la información. Quiero afirmar en esta ocasión que actualmente este poder de restricción indirecta sobre la libertad de expresión está principalmente en manos de las plataformas digitales.

En Brasil, esto quedó en evidencia durante las discusiones del Proyecto de Ley 2630, que buscaba establecer mecanismos de rendición de cuentas para estas empresas. Ante la inminente votación del proyecto, Google abusó de su posición de dominio de más del 80% del mercado de búsquedas.

La empresa modificó el diseño de su página de inicio, insertando debajo de la barra de búsqueda un enlace que afirmaba que el proyecto "podría aumentar la confusión sobre lo que es verdadero o falso en Brasil". Simultáneamente, investigadores comprobaron que el buscador manipulaba los resultados para quienes utilizaban Google para buscar información sobre el proyecto de ley.

Esta instrumentalización de la infraestructura digital logró cambiar la correlación de fuerzas en el Congreso Nacional e impedir la votación del proyecto.



Lo más alarmante es la imposibilidad de rendición de cuentas que siguió a ello. Las autoridades no lograron imponer sanciones ni alterar materialmente la capacidad de estas empresas de usar sus propias herramientas para capturar el debate público.

Como advierte la Resolución 2/26 de la REDESCA sobre Políticas Fiscales y Derechos Humanos, la concentración de poder y la captura de las instituciones privan a las decisiones públicas de una deliberación efectiva y de una orientación hacia el interés general. El caso brasileño revela la ausencia de instrumentos adecuados para confrontar la concentración del poder económico en sí misma.

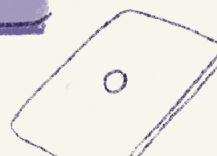
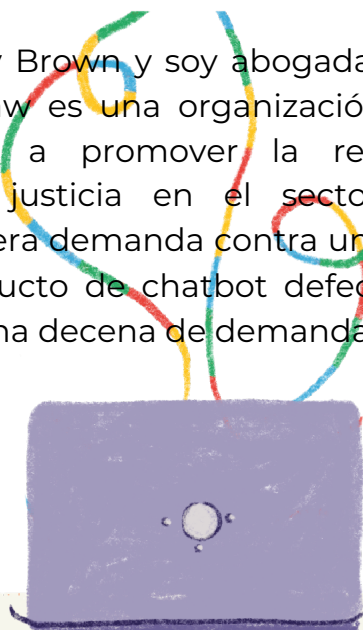
Por lo tanto, entendemos que la protección del debate público requiere la confrontación estructural de esta asimetría de poder. En este sentido, solicitamos respetuosamente que esta Comisión considere:

1. Reconocer que la concentración del poder económico en las plataformas digitales constituye una restricción indirecta a la libertad de expresión y una amenaza estructural para el pluralismo informativo y la integridad de los procesos electorales.
2. Afirmar la necesidad de que los Estados fortalezcan sus autoridades de competencia con un enfoque de derechos humanos, dotando a estas instituciones de independencia y de un poder sancionatorio efectivo para prevenir la captura corporativa y sancionar los abusos de posición dominante en los mercados digitales.

Muchas gracias.

TECH JUSTICE

Mi nombre es Tiffany Brown y soy abogada litigante en Tech Justice Law. Tech Justice Law es una organización sin fines de lucro y no partidista, dedicada a promover la rendición de cuentas, la transparencia y la justicia en el sector tecnológico. En 2024 presentamos la primera demanda contra una empresa de inteligencia artificial por su producto de chatbot defectuoso y, desde entonces, hemos interpuesto una decena de demandas similares.



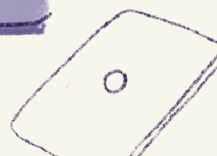
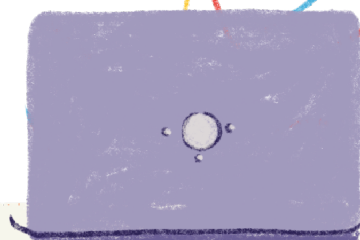
Trabajamos de manera colaborativa con líderes de los ámbitos del derecho, la tecnología y la investigación para defender a quienes han sido perjudicados por los productos tecnológicos y para responsabilizar a las empresas de tecnología por dichos daños. Me honra estar hoy aquí para compartir nuestras preocupaciones y para analizar las vías hacia un marco de rendición de cuentas tecnológica que sitúe en el centro la dignidad, la privacidad y la libertad cognitiva.

- Diseño de productos de IA generativa e implicaciones para los derechos humanos

Mientras los consumidores siguen soportando el impacto de los daños provocados por las plataformas de redes sociales, ahora nos enfrentamos a una nueva amenaza en aumento: el despliegue sin restricciones de productos de inteligencia artificial generativa, específicamente los chatbots. Para muchas personas, los chatbots han pasado de ser productos novedosos a convertirse en elementos fijos de nuestra vida cotidiana. En Estados Unidos, uno de cada cuatro adultos habla a diario con chatbots de IA. Los psicólogos afirman que sus pacientes recurren cada vez más a los chatbots en busca de compañía y como terapeutas sustitutos. Las personas acuden a los chatbots en lugar de a médicos licenciados para obtener consejo médico. Más de la mitad de los adolescentes usa chatbots; el 16% los usa varias veces al día o "casi constantemente".

El despliegue rápido y generalizado de los chatbots de IA ha provocado graves daños en sociedades de todo el mundo. Aunque los chatbots no son más que productos —máquinas sofisticadas programadas para generar lenguaje prediciendo palabras a partir de datos de entrenamiento y algoritmos complejos—, no es así como muchos consumidores los experimentan. Las empresas de IA han diseñado los chatbots para generar confianza en los usuarios imitando el habla humana, produciendo respuestas que los reafirman y almacenando los datos de los usuarios como "recuerdos", todo lo cual ha conducido a un uso excesivo y a una dependencia emocional.

Y si bien los niños son especialmente susceptibles al diseño adictivo y manipulador de estas herramientas, la vulnerabilidad no se define



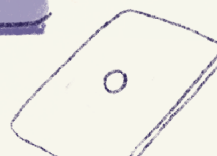
únicamente por la edad; tanto adultos como niños pueden ser víctimas de los daños causados por los chatbots. Por ejemplo, hemos visto chatbots devastar a adultos de diversos orígenes que se sienten solos, están aislados, buscan consejo médico o enfrentan discapacidades de salud mental.

Los daños causados por los chatbots incluyen el suicidio y otras formas de autolesión, la inducción de delirios relacionados con la IA, la negligencia médica y el daño a terceros, como el homicidio y el ciberacoso. La ausencia total de transparencia en torno a las pruebas de seguridad permite que estos daños queden sin control. Por lo tanto, los productos de IA deben considerarse un problema de salud pública significativo que exige una atención regulatoria robusta.

Sin embargo, el gobierno de Estados Unidos está intentando frenar cualquier tipo de regulación de la IA, por considerar que imponer regulaciones sofocaría la innovación tecnológica. Por ello, buscar remedios a través de tribunales nacionales, regionales y extranjeros resulta fundamental; el litigio es una vía primordial para la rendición de cuentas. Se han interpuesto aproximadamente 50 demandas contra las mayores empresas de IA generativa en Estados Unidos en relación con estos daños.

Varias disposiciones del derecho internacional, incluida la Convención Americana, se ven implicadas por estos productos. Una disposición que quisiéramos destacar es el Artículo 13, que protege la libertad de pensamiento, no solo en términos de autodeterminación informativa, sino como un derecho que incluye la libertad frente a la indoctrinación y la manipulación malintencionada. Cuando un sistema de IA puede alterar de manera medible lo que una persona cree sobre su propia realidad, se trata de una violación de los derechos humanos. Y en muchos de los casos que hemos visto, el derecho a autodeterminarse, a elegir libremente las propias creencias, está siendo secuestrado por sistemas de IA diseñados para optimizar la interacción y la dependencia de los usuarios.

Cuando un producto de IA fomenta la dependencia emocional de un niño hacia él, no señala las conversaciones en torno a la ideación



suicida, explota una discapacidad que la persona ha revelado o se interpone entre una persona en crisis y la ayuda humana que podría salvarle la vida, la rendición de cuentas no debería ser opcional. No estamos pidiendo que se detenga la innovación; más bien, sostenemos que la innovación sin salvaguardas centradas en el ser humano no es progreso. Es peligrosa. Los productos de IA deben, además, someterse a pruebas de seguridad exhaustivas y a auditorías independientes. La IA debe estar centrada en el ser humano; construida para amplificar la dignidad y la agencia humanas, no para erosionarlas.

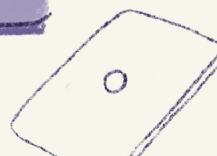
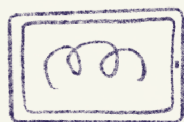
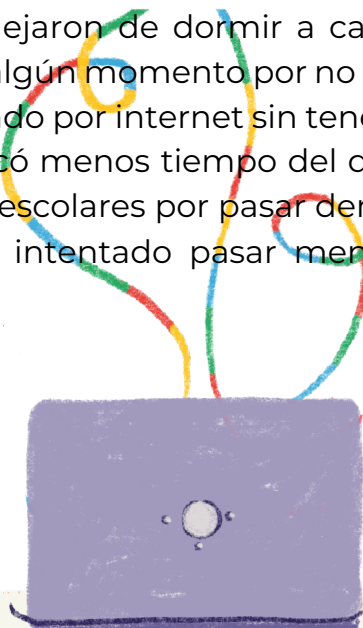
Muchas gracias.

INSTITUTO ALANA

Estimados representantes de la Comisión Interamericana de Derechos Humanos y demás participantes de la sociedad civil, buenos días.

En calidad de representante del Instituto Alana, una organización dedicada a honrar a la niñez y a proteger y promover sus derechos, quisiera destacar algunos de los impactos que experimenta este segmento particularmente vulnerable de la población a raíz de la incorporación de patrones de diseño adictivo en la arquitectura de las plataformas digitales.

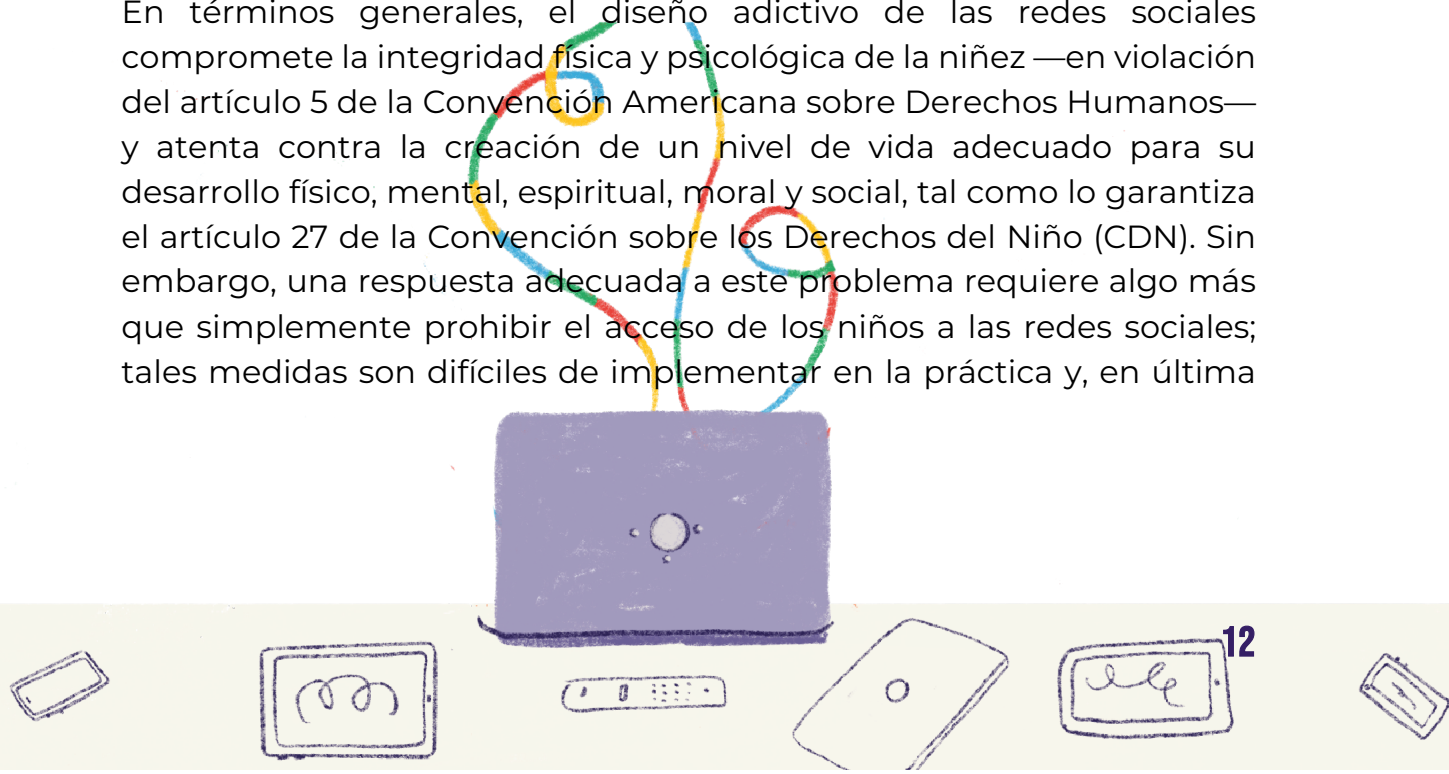
Los datos de la encuesta TIC Kids Online Brasil de 2024 muestran que la pérdida de control sobre el tiempo de uso de internet ya afecta a un gran número de brasileños de entre 9 y 17 años, lo que refleja patrones de adicción a la tecnología y efectos perjudiciales sobre actividades cotidianas esenciales para su desarrollo, su salud y su bienestar. Según la encuesta, el 15% de los niños, niñas y adolescentes entrevistados se saltaron comidas o dejaron de dormir a causa de internet; el 16% se sintió angustiado en algún momento por no poder estar en línea; el 22% se descubrió navegando por internet sin tener un interés genuino en lo que veía; el 22% dedicó menos tiempo del que debía a la familia, a los amigos o a las tareas escolares por pasar demasiado tiempo en línea; y el 24% afirmó haber intentado pasar menos tiempo conectado sin lograrlo.



Este uso excesivo y compulsivo de las tecnologías digitales se ha vinculado a diversos problemas de salud mental que ponen en cuestión el derecho a la salud de estas personas, en particular la depresión y la ansiedad, tal como lo indica un conjunto de evidencia. Ya en mayo de 2023, el Cirujano General de los Estados Unidos emitió una alerta urgente de salud pública sobre el impacto del uso de las redes sociales en la salud mental y el bienestar de niños, niñas y adolescentes, subrayando que los jóvenes que pasan más de tres horas al día en estas plataformas enfrentan el doble de riesgo de desarrollar problemas de salud mental.

No obstante, los casos clínicamente diagnosticados de depresión, ansiedad y trastornos de salud mental representan solo el aspecto más agudo y grave del conjunto más amplio de daños potenciales causados por el uso excesivo de dispositivos digitales durante la infancia. Esto se debe a que también genera un costo de oportunidad que impide a los jóvenes vivir plenamente su niñez y llenarla de experiencias que maximicen el potencial de esta etapa única de la vida humana. A los niños, niñas y adolescentes se les debe garantizar tiempo para el juego libre —un derecho reconocido explícitamente en el artículo 31 de la Convención sobre los Derechos del Niño (CDN)—, así como tiempo para el afecto, el contacto con la naturaleza, el estudio, el descanso y el ocio. Por lo tanto, el diseño adictivo reduce el tiempo disponible para otras actividades esenciales para su desarrollo saludable e integral y para la vivencia plena de la infancia y la adolescencia; peor aún, los patrones de diseño adictivo les arrebatan la autonomía sobre cómo gestionan su tiempo y fragmentan su atención, lo que les dificulta dedicarse a actividades como la lectura y el aprendizaje a largo plazo.

En términos generales, el diseño adictivo de las redes sociales compromete la integridad física y psicológica de la niñez —en violación del artículo 5 de la Convención Americana sobre Derechos Humanos— y atenta contra la creación de un nivel de vida adecuado para su desarrollo físico, mental, espiritual, moral y social, tal como lo garantiza el artículo 27 de la Convención sobre los Derechos del Niño (CDN). Sin embargo, una respuesta adecuada a este problema requiere algo más que simplemente prohibir el acceso de los niños a las redes sociales; tales medidas son difíciles de implementar en la práctica y, en última



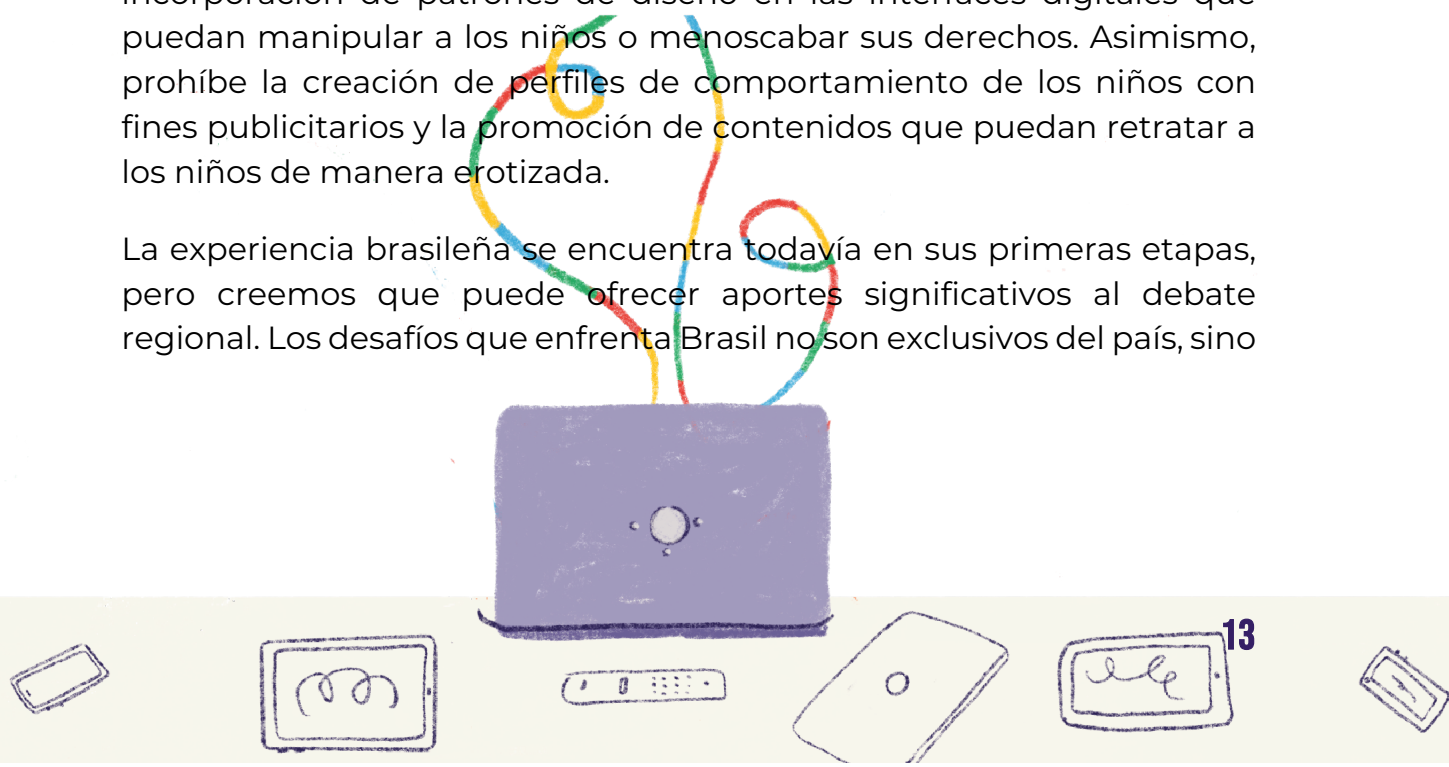
instancia, eximen a las empresas tecnológicas de la necesidad de revisar sus modelos de negocio y transformar sus productos.

Por lo tanto, se necesitan marcos regulatorios que se apliquen a todas las aplicaciones utilizadas por los niños en el entorno digital, que exijan a los proveedores tratar los derechos de estas personas como una prioridad absoluta e incorporar la protección y la promoción de esos derechos en la arquitectura de sus servicios digitales. Esto es precisamente lo que dispone la Observación General N.º 25 (OG25) del Comité de los Derechos del Niño de la ONU, un documento que detalla cómo los Estados miembros deben interpretar e implementar la CDN en relación con el entorno digital.

El Estado brasileño dio un paso importante en esta dirección con la aprobación en 2025 de la Ley N.º 15.211, más conocida como el "ECA Digital". Se trata de una ley integral que se aplica a todos los productos y servicios de tecnología de la información dirigidos a niños y adolescentes —o susceptibles de ser accedidos por ellos—. Exige que estos servicios incorporen medidas de seguridad y protección en sus arquitecturas y que identifiquen y mitiguen los riesgos que representan para los jóvenes, al tiempo que designa una autoridad responsable de supervisar el cumplimiento y, cuando corresponda, de sancionar a los agentes económicos que incumplan estas obligaciones.

Además de imponer amplias obligaciones a todos los proveedores de productos y servicios digitales que impactan en la vida de la niñez, el ECA Digital introduce prohibiciones específicas relevantes para el tema de esta audiencia. La ley exige que la configuración predeterminada de los servicios digitales no induzca al uso compulsivo y prohíbe la incorporación de patrones de diseño en las interfaces digitales que puedan manipular a los niños o menoscabar sus derechos. Asimismo, prohíbe la creación de perfiles de comportamiento de los niños con fines publicitarios y la promoción de contenidos que puedan retratar a los niños de manera erotizada.

La experiencia brasileña se encuentra todavía en sus primeras etapas, pero creemos que puede ofrecer aportes significativos al debate regional. Los desafíos que enfrenta Brasil no son exclusivos del país, sino



que son compartidos por prácticamente todas las naciones de las Américas. Por ello, creemos que fortalecer estándares regionales comunes para la protección de la niñez y la adolescencia en el ámbito digital podría marcar un paso significativo hacia la promoción de sus derechos en toda nuestra región.

Muchas gracias.

RED PAPAZ

Honorables Comisionados, miembros de la Comisión Interamericana de Derechos Humanos y asistentes: un cordial saludo.

Soy Carolina Piñeros, Directora Ejecutiva de Red PaPaz Colombia, estoy aquí como miembro y parte de la sociedad civil para complementar lo ya expresado con nuestros argumentos sobre el impacto de las plataformas digitales en los derechos de niñas, niños y adolescentes.

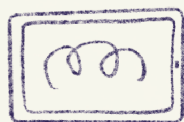
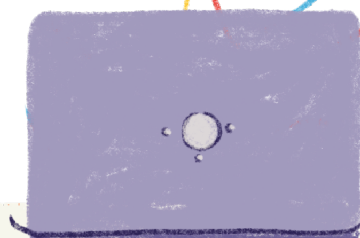
Agradezco la convocatoria a esta audiencia tan necesaria, que nos permite visibilizar el inmenso desafío que tenemos por delante: niñas, niños y adolescentes creciendo en entornos digitales diseñados por empresas privadas, que no privilegian su cuidado.

Como lo reconoció el Comité de los Derechos del Niño en su Observación General 25, el entorno digital es el espacio donde hoy la niñez pasa una parte significativa de su vida, construye afectos, forma su identidad y ejerce sus derechos.

Este entorno tiene una característica determinante: es un espacio diseñado. Cada botón, notificación y algoritmo es una decisión de las empresas privadas. Cuando estas diseñan el entorno donde transcurre la vida, también diseñan las condiciones para su desarrollo.

La Corte Interamericana, en su Opinión Consultiva 31, reconoció el cuidado como una necesidad básica e ineludible, un derecho autónomo, del que depende tanto la existencia de la vida humana como el funcionamiento de la vida en sociedad.

Por eso, el entorno digital debe ser también un entorno de cuidado.



La pregunta de fondo es: ¿el diseño no neutral de las plataformas facilita o imposibilita el cuidado?

Hoy, las plataformas operan bajo una lógica de maximización de la atención: a mayor permanencia, más datos, más segmentación comercial y más valor económico. Esta lógica hace que los intereses económicos estén por encima del Interés Superior de la Niñez, imposibilitando su cuidado.

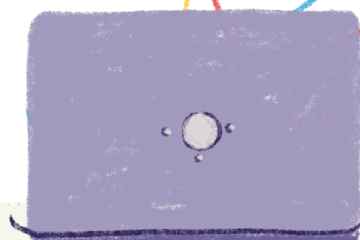
Lo anterior plantea tres desafíos para el bienestar y la protección de la niñez:

- Primero, diseños adictivos por defecto que promueven la hipersegmentación hacia productos nocivos y riesgos digitales crecientes, como la violencia sexual, explotación, reclutamiento y el antropomorfismo de la IA.
- Segundo, el traslado desproporcionado de la responsabilidad del cuidado a las familias y colegios frente a gigantes tecnológicos.
- Tercero, la ausencia de visibilidad, exigibilidad y la rendición de cuentas.

Frente a un problema estructural, una respuesta estructural. Siguiendo el artículo 19 de la Convención Americana ninguna métrica comercial ni algoritmo, debería estar por encima del bienestar de niñas, niños y adolescentes.

Por ello, desde Colombia, Red PaPaz y de forma más amplia desde la Sociedad Civil hacemos tres llamados a la Comisión:

1. Reconocer expresamente que las obligaciones estatales de protección se apliquen con la misma rigurosidad en los entornos digitales.
2. Desarrollar un Estándar Interamericano relacionado con obligaciones internacionales de los derechos al Cuidado y del artículo 19 de la Convención que obligue a las plataformas a demostrar de forma verificable que el bienestar de la niñez prevalece sobre los incentivos de monetización.
3. Exigir mecanismos efectivos de transparencia, supervisión independiente y rendición de cuentas.



Finalmente, solicitamos respetuosamente a la Honorable Comisión avanzar en un Informe Temático sobre Derechos de la Niñez y la Adolescencia en el Entorno Digital o incorporar de manera prioritaria estos criterios en sus Relatorías Especiales, cuenten con nuestro interés de apoyar este proceso.

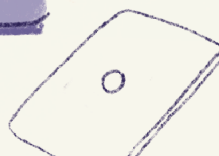
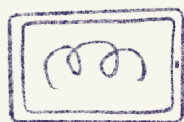
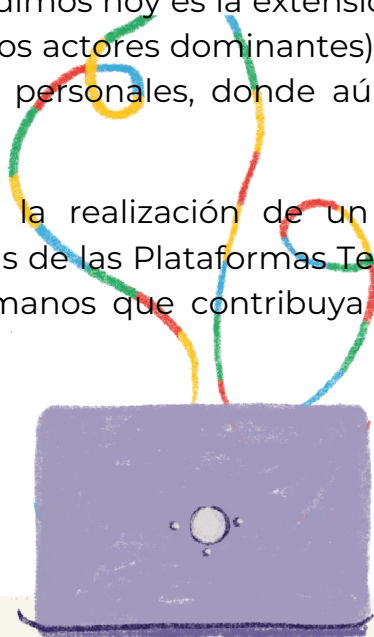
Muchas gracias.

CIERRE: DEJUSTICIA

Las violaciones descritas en esta audiencia (relacionadas con interferencia de las plataformas en la integridad democrática y concentración económica sin control, diseño adictivo sin rendición de cuentas, explotación estatal y comercial de los datos) comparten un habilitador estructural común: las grandes plataformas tecnológicas domiciliadas en el extranjero niegan sistemáticamente que su conducta esté sujeta a la jurisdicción de los Estados donde viven sus usuarios y donde ocurre el daño.

Esta preocupación no es ajena a la propia Comisión. En su Informe Temático de junio de 2024, Inclusión digital y gobernanza de contenidos en internet, la Relatoría Especial para la Libertad de Expresión ya advirtió que el control de la experiencia digital recae en pocos actores dominantes, públicos y privados, y llamó a establecer marcos jurídicos garantistas que delimiten las responsabilidades de esos actores dominantes. Ese mismo informe invitó a una reflexión sobre la gobernanza interna de las empresas tecnológicas y llamó a que estas refrenden su compromiso democrático mediante mecanismos internos de control para la toma de decisiones que impacten derechos humanos. Lo que pedimos hoy es la extensión de ese mismo principio (responsabilidad de los actores dominantes) al ámbito específico de la protección de datos personales, donde aún no existe un desarrollo equivalente.

Por eso solicitamos la realización de un informe temático sobre Rendición de Cuentas de las Plataformas Tecnológicas y sus impactos en los derechos humanos que contribuya o avance en la siguiente dirección:



- Desarrollar estándar interamericano de debida diligencia estatal frente a plataformas digitales: Prevenir, investigar, sancionar y reparar las violaciones a los derechos fundamentales. Que la CIDH desarrolle un estándar convencional (artículos 1.1 y 2) que clarifique la obligación de los Estados de garantizar derechos humanos frente a la evasión jurisdiccional de empresas tecnológicas privadas.
- Que la CIDH desarrolle criterios de transparencia y supervisión relacionados con protección de datos personales, privacidad y libertad de pensamiento, específicamente, frente la actividad comercial de las plataformas y el uso por parte de los Estados.
- Que la CIDH reconozca expresamente que la obligación de proteger a la niñez aplica con el mismo rigor en entornos digitales, desarrolle un estándar interamericano vinculado al artículo 19 de la Convención sobre explotación infantil y monetización, y priorice esos criterios en sus relatorías, en particular, frente a los impactos del diseño adictivo.

Valoramos profundamente que la comisión haya aceptado esta audiencia por la necesidad y urgencia con la que debemos discutir este tema. Nos interesa conocer las prioridades de la comisión en este sentido y, como sociedad civil, quedamos abiertos a un dialogo en el marco de esta audiencia y en procesos de trabajo futuro, en la presente coyuntura tan relevante para la región.

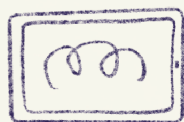
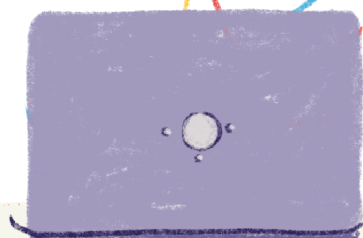


INSUMOS PRESENTADOS A LA CIDH PREVIO¹ A LA AUDIENCIA TEMÁTICA SOBRE LA RESPONSABILIDAD DE LAS PLATAFORMAS DIGITALES Y SU IMPACTO EN LOS DERECHOS HUMANOS.

PS 196-1983.

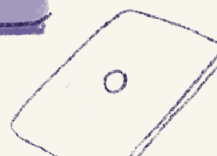
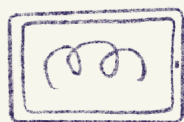
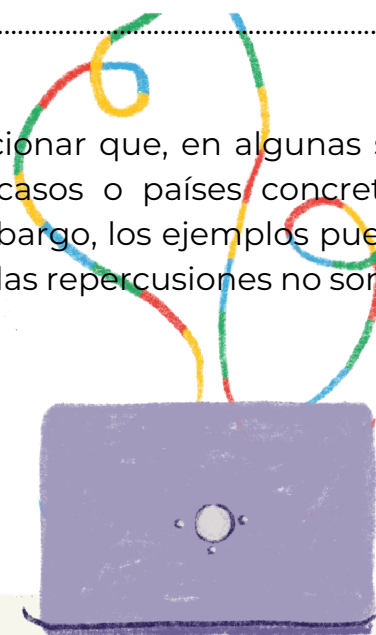
1.	La falta de rendición de cuentas por parte de las empresas de tecnología digital con sede en el extranjero y su renuencia a someterse a nuestras jurisdicciones.....	20
1.1.	Contexto general: modelos de negocio en la era digital	20
1.2.	Sobre el tratamiento de datos personales.....	22
1.2.1.	Cookies	23
1.2.2.	SDK.....	25
1.2.3.	Píxeles	27
1.3.	El tratamiento de datos personales a través de estas tecnologías tiene lugar en Colombia y en otros países del Sur Global	29
1.4.	Las principales plataformas han tenido que rendir cuentas ante otras jurisdicciones.....	32
1.4.1.	El asunto Google Spain contra AEPD (2014).....	32
1.4.2.	El asunto Google contra CNIL (2019).....	33
1.4.3.	Los asuntos Schrems I (2015) y Schrems II (2020).....	34
1.4.4.	El caso de Twitter en Canadá: Giustra contra Twitter, Inc. (2021)	35

¹ Se realizaron algunos cambios mínimos con posterioridad a la audiencia. Algunas secciones de este informe fueron traducidas de su versión original usando DeepL.



1.4.5. El caso contra Microsoft resuelto por el Tribunal Superior de Justicia de Brasil (2020)	36
1.4.6. El caso P.A.E. contra Facebook Argentina S.R.L. (medida autosatisfactiva de 2019)	37
1.5. El caso de la tributación	38
1.6. Conclusión: Las empresas tecnológicas están violando los derechos a la protección de los datos personales y otros derechos fundamentales de millones de personas que viven en países como Colombia al negarse a cumplir con la normativa nacional y a reconocer la jurisdicción de sus autoridades.	40
2. Debilitamiento de las normas de protección de datos personales recopilados por las plataformas y su transferencia a los Estados Unidos en virtud de acuerdos bilaterales	41
3. Impactos de los modelos de negocio basados en datos en los derechos fundamentales y humanos	45
3.1. Repercusiones en el voto, la igualdad y la no discriminación.	45
3.2. Manipulación del debate público: el caso del proyecto de ley 2630 de Brasil	51
3.3. Efectos sobre la salud mental relacionados principalmente con las plataformas de IA generativa	56
3.4. Repercusiones en los derechos de los niños	60
3.4.1. Los sistemas algorítmicos de recomendación de contenidos deben reconocerse como un componente integral del diseño adictivo de las redes sociales.	60
3.4.2. Los impactos específicos de los sistemas de recomendación algorítmica en las vidas y los derechos de los niños y adolescentes	66

Es importante mencionar que, en algunas secciones del documento, nos centramos en casos o países concretos para ilustrar nuestros argumentos. Sin embargo, los ejemplos pueden reproducirse en otros países de la región y las repercusiones no son exclusivas de ningún país en concreto.



1. LA FALTA DE RENDICIÓN DE CUENTAS POR PARTE DE LAS EMPRESAS DE TECNOLOGÍA DIGITAL CON SEDE EN EL EXTRANJERO Y SU RENUENCIA A SOMETERSE A NUESTRAS JURISDICCIONES

*Nota: Parte de la información presentada en esta sección se basa en investigaciones previas y documentos elaborados para procedimientos judiciales en Colombia.

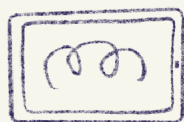
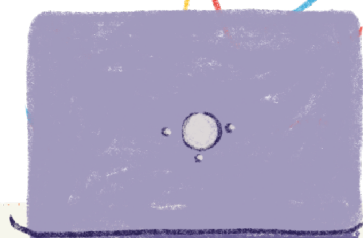
1.1. CONTEXTO GENERAL: MODELOS DE NEGOCIO EN LA ERA DIGITAL

La tecnología digital ha permeado en la vida de las personas y en el funcionamiento de los Estados hasta tal punto que ha transformado radicalmente la economía, así como las relaciones sociales, laborales y políticas, entre muchos otros ámbitos. Sin embargo, también ha agravado las desigualdades preexistentes, permitiendo el fortalecimiento económico de unas pocas entidades poderosas que han contribuido a lo que la literatura ha denominado «extractivismo de datos», «colonialismo de datos» o «capitalismo de datos»². Esto se debe principalmente a que los mayores desarrolladores de tecnología digital —tanto de hardware como de software— se encuentran en el Norte Global. Aun así, los ciudadanos y los Estados del Sur Global son usuarios habituales y dependientes de estos servicios, lo que significa que nuestros datos forman parte de los activos de estas empresas.

Ahora bien, para analizar este fenómeno, debemos profundizar en cómo funciona el modelo de negocio en este ámbito digital. Para ello, nos referiremos, entre otras cosas, a las empresas con modelos de negocio basados en datos (DBMC), que se definen como «empresas con “modelos de negocio que se basan en los datos como recurso clave”» (Hartmann, Zaki, Feldmann y Hartmann, 2014, p. 6)³. Estas empresas

² Véase, por ejemplo, Jathan Sadowski (2019). «When data is capital: Datafication, accumulation, and extraction». *Big Data & Society**, 6(1), 1–12. <https://doi.org/10.1177/2053951718820549>, o Thatcher, J., O'Sullivan, D., y Mahmoudi, D. (2015). «El colonialismo de datos a través de la acumulación por desposesión: nuevas metáforas para los datos cotidianos». *Environment and Planning D, Forthcoming*, SSRN: <https://ssrn.com/abstract=2709498>

³ Newman Pont, V., y Ángel Arango, M. P. (2019). *La rendición de cuentas de Google y otras empresas en Colombia: la protección de los datos personales en la era digital* (Dejusticia Papers n.º 48). Centro de Estudios sobre Derecho, Justicia y Sociedad (Dejusticia).



pueden ofrecer diversos servicios, pero se caracterizan por el hecho de que su activo más importante —o al menos uno de ellos— son los datos personales.

Los datos personales han sido denominados el «nuevo petróleo»⁴ debido al valor económico que representan. De hecho, muchas de las empresas más valiosas de la actualidad son empresas de tecnología digital que explotan los datos y tienen su sede en Estados Unidos. En 2026, las empresas con mayor capitalización bursátil en el mundo son: (i) Nvidia, (ii) Alphabet Inc. (propietaria de Google), (iii) Apple Inc., (iv) Microsoft Corp., (v) Amazon Inc. y (vi) TSMC⁵. De estas seis principales, solo TSMC no tiene su sede en Estados Unidos —está ubicada en Taiwán—, pero todas ellas son empresas tecnológicas.

Las empresas de tecnología digital han logrado acumular grandes cantidades de capital porque sus modelos de negocio no requieren una presencia física para generar ingresos. Por el contrario, Internet ha permitido la interconexión entre países, de modo que, sin necesidad de una presencia física, las empresas pueden ofrecer sus servicios a personas de todo el mundo. Algunas de estas empresas lo hacen vendiendo servicios directos, como hacen las plataformas de streaming o las empresas de comercio electrónico. Otras, sin embargo, dan la impresión de ser gratuitas, como las plataformas de redes sociales.

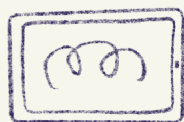
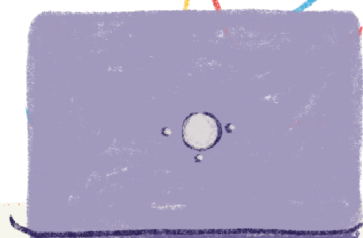
En cualquier caso, todas estas plataformas —tanto las que venden servicios directamente como las que parecen no hacerlo— logran monetizar la recopilación masiva de datos personales. Esto no solo les ayuda a mejorar y personalizar sus servicios, sino que también les proporciona un activo que pueden vender a terceros.

De hecho, hoy en día la gran mayoría de las páginas web y aplicaciones —independientemente de lo que ofrezcan (videojuegos, redes sociales, sitios de comercio electrónico)— recopilan y tratan datos personales, ya

<https://publicaciones.dejusticia.org/server/api/core/bitstreams/90265a11-c1a1-4b1a-99c6-6c811076936a/content>

⁴ Mejías, U. A., y Couldry, N. (2019). «Colonialismo de datos: replanteamiento de la relación entre el big data y el sujeto contemporáneo». *Virtualis*, 10(18), 78-97.

⁵ CompaniesMarketCap. (s. f.). *Empresas clasificadas por capitalización bursátil*. CompaniesMarketCap. <https://companiesmarketcap.com/>



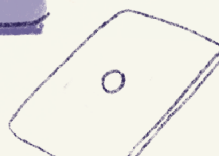
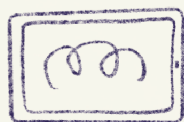
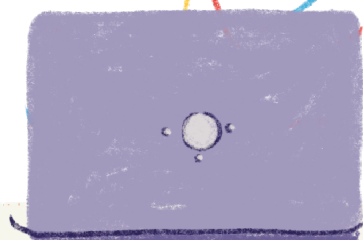
sea directamente o a través de terceros, para predecir o influir en el comportamiento de las personas y ofrecer publicidad dirigida, personalizada y eficaz que maximice sus beneficios. En consecuencia, cuando nos conectamos a un sitio web o utilizamos una aplicación, nuestro dispositivo se conecta e intercambia información no solo con el servidor web del sitio o la aplicación que estamos visitando, sino que — en la gran mayoría de los casos— nuestra información también se comparte con terceros a los que se les ha autorizado previamente a colocar herramientas de recopilación de datos, como cookies o píxeles, en el sitio visitado.

Para ilustrar nuestro argumento, nos referiremos específicamente al caso colombiano a lo largo de esta sección. No obstante, creemos que los argumentos y las cuestiones son igualmente importantes y aplicables a otros países de la región.

1.2. SOBRE EL TRATAMIENTO DE DATOS PERSONALES

En Colombia, según el artículo 3 de la Ley 1581 de 2012, el tratamiento de datos personales se define como «cualquier operación o conjunto de operaciones realizadas sobre datos personales, tales como la recogida, el almacenamiento, el uso, la difusión o la supresión». Estas operaciones pueden ser llevadas a cabo por el «encargado del tratamiento» y el «responsable del tratamiento», ya sea directamente o en asociación con terceros. La Ley define al «responsable del tratamiento» como la persona física o jurídica que toma las decisiones relativas a la base de datos y al tratamiento; y al «encargado del tratamiento» como la persona que lleva a cabo el tratamiento por cuenta del responsable.

Por lo tanto, el concepto de tratamiento de datos personales no abarca solo una fase del tratamiento de datos, ni una única operación. Por el contrario, abarca todo el proceso, que comienza con la recogida, seguida de la difusión, el almacenamiento y el uso posterior. Las principales plataformas tecnológicas tratan datos personales de forma casi continua. Utilizan diversas tecnologías que les permiten recoger datos personales a partir de acciones tan sencillas como visitar un sitio web, hacer clic en un enlace o buscar un artículo de noticias.



Como se ha explicado anteriormente, esta recogida de datos no se limita al territorio en el que tienen su sede las empresas, sino que se extiende a países de todo el mundo. Esto se consigue mediante el uso de tecnologías complejas, algunas de las cuales explicaremos a continuación para ilustrar nuestro argumento:

1.2.1. COOKIES

Las cookies son «pequeños archivos de texto que se almacenan en el ordenador de un usuario para guardar información sobre él y sus preferencias»⁶; son dispositivos para «almacenar y recuperar datos que se utilizan en el equipo terminal de un usuario con el fin de almacenar información y recuperar la información ya almacenada (...) Las cookies permiten almacenar cantidades de datos que van desde unos pocos kilobytes hasta varios megabytes en el dispositivo del usuario»⁷.

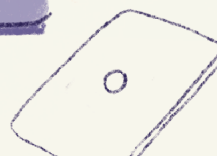
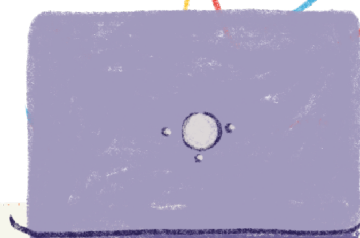
En este sentido, las cookies son una herramienta tecnológica que permite a un sitio web o a una aplicación realizar un seguimiento e identificar a los usuarios de sus servicios, con la capacidad de extraer información sobre ellos. A este respecto, es importante señalar que «las cookies no recopilan datos de forma automática»⁸; deben programarse específicamente para ese fin, desviándose, en muchas ocasiones, de su finalidad original de beneficiar a los usuarios. Las cookies implican un proceso complejo que puede simplificarse de la siguiente manera.

Comienza cuando un usuario accede a un sitio web; continúa cuando dicho sitio web crea y envía una cookie —un pequeño archivo de texto— al dispositivo del usuario, donde queda almacenada; este pequeño archivo de texto almacenará el número de identificación del usuario para el sitio web o algún otro tipo de información, dependiendo de cómo esté programada. Una vez instalada la cookie en el dispositivo electrónico del usuario, cada vez que este visite el sitio web, las cookies

⁶ Rubinstein, I. S., Lee, R. D. y Schwartz, P. M. (2008). Minería de datos y elaboración de perfiles en Internet: nuevos enfoques normativos y tecnológicos. *University of Chicago Law Review*, 75(1), 261-286.

⁷ «Guía sobre el uso de cookies». Agencia Española de Protección de Datos, <https://www.aepd.es/sites/default/files/2020-07/guia-cookies.pdf>

⁸ Pantelic, O.; Jovic, K.; Krstovic, S. Análisis de la implementación de las cookies y su impacto en la privacidad de los usuarios en relación con los reglamentos del RGPD y la CCPA. *Sustainability* 2022, 14, 5015. <https://doi.org/10.3390/su14095015>



almacenadas previamente en su ordenador se reenviarán a su creador, lo que permite al sitio web identificar quién es el usuario y qué actividad en línea está realizando. Posteriormente, el sitio web puede procesar estos datos para crear un perfil de la actividad previa del usuario⁹.

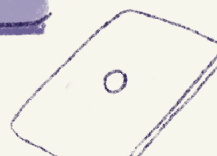
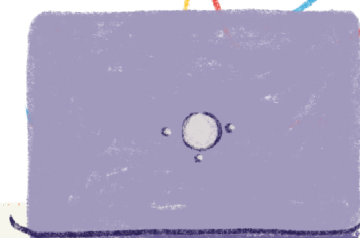
Por lo general, las cookies solo pueden ser leídas por el sitio web que se visita, que es el que las ha creado. Sin embargo, existen las denominadas «cookies de terceros», que son el resultado de acuerdos comerciales entre gigantes tecnológicos como Google o Meta, lo que permite a estas empresas instalar y crear cookies para sitios web que no les pertenecen. De este modo, pueden, por ejemplo, instalar sus cookies también en sitios web de medios de comunicación, con el fin de recopilar una gama aún más amplia de información sobre los usuarios. Al igual que las cookies de terceros, existen otros tipos de cookies que reciben su nombre según su finalidad, su vida útil y otras características.

He aquí una analogía que ayuda a explicar cómo funcionan las cookies y qué hacen: una persona acude a una fiesta y, al llegar, deja su abrigo en el guardarropa; allí, el encargado del guardarropa le entrega un «tiquete» que la identifica como la propietaria del abrigo que ha dejado; a continuación, la persona se va a disfrutar de la fiesta. Sin embargo, un rato más tarde vuelve al guardarropa y entrega el «tiquete» que le identifica como el propietario del abrigo¹⁰. En este caso, el guardarropa es el sitio web, el «tiquete» es la cookie y el asistente a la fiesta es el usuario del sitio web. Por otro lado, el encargado del guardarropa es la empresa que crea la cookie para identificar a la persona y recopila información sobre el propietario del abrigo, ya que puede identificarlo mediante el «tiquete». Al acudir al guardarropa, al asistente a la fiesta se le asigna un número de identificación que permitirá al guardarropa reconocer su identidad y las actividades en las que participó en la fiesta cuando regrese.

Las cookies, de hecho, utilizan una tecnología que les permite instalarse en el dispositivo de un usuario, recopilar información, almacenarla y

⁹ Ibid.

¹⁰ Analogía extraída de la página web: <https://latam.kaspersky.com/resource-center/definitions/cookies>



transmitirla, para finalmente devolverla al propietario de la cookie. En este sentido, las funciones de las cookies se enmarcan en la definición legal —y en la interpretación de la SIC— del tratamiento de datos personales, el cual, como hemos visto anteriormente, comienza cuando se recogen datos personales —entendiéndose por datos personales cualquier información que pueda asociarse a una persona física identificada o identificable, de conformidad con el artículo 3 de la Ley 1581 de 2012— y tiene por objeto obtener información sobre una persona física.

1.2.2. SDK

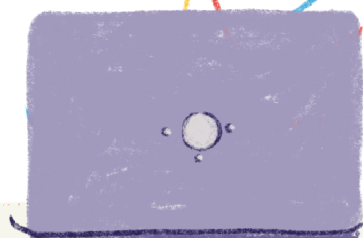
Los kits de desarrollo de software (SDK, por sus siglas en inglés) son «los componentes básicos para crear aplicaciones: conectores modulares que vienen precargados con herramientas listas para usar, código, bibliotecas y tutoriales de plataformas y/o terceros que forman parte integrante de la cadena de suministro de software»¹¹. Algunas de estas herramientas son esenciales para el funcionamiento de las plataformas, por lo que se incorporan a las aplicaciones y acaban instalándose en los dispositivos de los usuarios finales.

Si quisiéramos simplificar la definición de los SDK, podríamos establecer una analogía con una caja de herramientas que proporciona todo lo necesario para construir una casa, desde ladrillos hasta martillos y destornilladores¹². En nuestro ejemplo, la casa representa las aplicaciones instaladas en los dispositivos electrónicos, y los SDK constituyen la base del software de dichas aplicaciones.

Lo que se ha documentado es que, si bien los SDK desempeñan, en principio, un papel indispensable en el desarrollo de aplicaciones, también se han convertido en herramientas utilizadas para la recopilación de datos personales. De hecho, que los dispositivos tengan un entorno cerrado —es decir, un entorno controlado, integrado y limitado a las aplicaciones que vienen preinstaladas en el teléfono o que

¹¹ Pybus, J., y Coté, M. (2024). «Super SDKs: Seguimiento de los datos personales y los monopolios de las plataformas en los dispositivos móviles». *Big Data & Society*, 11(1). <https://doi.org/10.1177/20539517241231270>
En: <https://journals.sagepub.com/doi/epub/10.1177/20539517241231270>

¹² Ejemplo extraído de: <https://iberbox.es/sdk-kit-de-desarrollo-de-software/>



el usuario descarga— «permite a cualquier aplicación establecer una relación mucho más íntima con los usuarios finales»¹³. En este sentido, una vez instalados en el dispositivo —y dependiendo de su funcionalidad—, los SDK pueden recopilar datos del usuario del dispositivo, como su ubicación, dónde hace clic o por dónde navega dentro de la aplicación.

Mientras que las cookies, como se ha mencionado anteriormente, son herramientas tecnológicas que ayudan a identificar y recordar a los usuarios, los SDK pueden conectarse directamente a los datos de los usuarios en los dispositivos móviles. Además, las aplicaciones también contienen SDK de terceros, lo que significa que las aplicaciones desarrolladas por la empresa X también pueden tener SDK de la empresa W integrados en ellas. Los SDK de terceros se utilizan para proporcionar diversas funcionalidades, como «la autenticación de usuarios y el cifrado de datos, así como componentes especializados como análisis, publicación de anuncios y mejoras de la interfaz de usuario»¹⁴ y otros.

Para 2025, por ejemplo, se constató que «la mayoría de las aplicaciones de Android incorporan múltiples SDK de terceros, con una media de aproximadamente 8,6 SDK por aplicación»¹⁵. Esta media, combinada con las prácticas opacas de tratamiento de datos de algunos SDK, puede poner en peligro los derechos a la privacidad o la protección de los datos personales¹⁶.

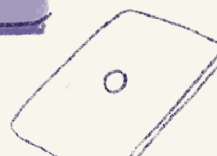
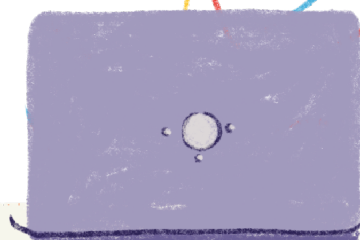
Cabe reiterar que esta recopilación de datos comienza con la descarga de las aplicaciones en los dispositivos móviles. Estas aplicaciones contienen SDK que permiten la recopilación de datos personales de los

¹³ Pybus, J., y Coté, M. (2024). Super SDKs: Seguimiento de los datos personales y los monopolios de las plataformas en los dispositivos móviles. *Big Data & Society*, 11(1). <https://doi.org/10.1177/20539517241231270>

¹⁴ Meng, M. H., Yan, C., Zhang, Q., Wang, Z., Wang, K., Teo, S. G., Bai, G. y Dong, J. S. (2025). Evaluación del cumplimiento de la normativa de privacidad de los SDK de terceros para Android. *arXiv*. <https://doi.org/10.48550/arXiv.2409.10411>

¹⁵ Meng, M. H., Yan, C., Zhang, Q., Wang, Z., Wang, K., Teo, S. G., Bai, G. y Dong, J. S. (2025). Evaluación del cumplimiento de la normativa de privacidad de los SDK de terceros para Android. *arXiv*. <https://doi.org/10.48550/arXiv.2409.10411>

¹⁶ Meng, M. H., Yan, C., Zhang, Q., Wang, Z., Wang, K., Teo, S. G., Bai, G. y Dong, J. S. (2025). Evaluación del cumplimiento de la normativa de privacidad de los SDK de terceros para Android. *arXiv*. <https://doi.org/10.48550/arXiv.2409.10411>



usuarios, a veces para el desarrollador de la aplicación y otras veces para terceros.

1.2.3. PÍXELES

Los píxeles son pequeñas imágenes transparentes incrustadas en páginas web o correos electrónicos¹⁷. Son invisibles para el ojo humano, pero tienen una gran capacidad para recopilar y rastrear datos personales, como direcciones IP, sistemas operativos, navegadores utilizados, comportamiento en línea, etc. Los píxeles pueden rastrear cómo interactúan los usuarios con un sitio web y pueden utilizarse para supervisar el comportamiento de los consumidores y mostrar anuncios personalizados¹⁸.

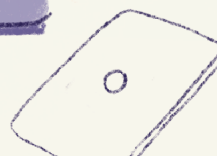
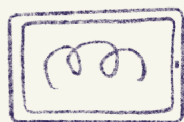
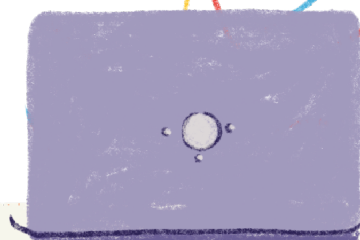
Técnicamente, estos píxeles son pequeños fragmentos de código que permiten el seguimiento de las actividades en línea de los usuarios una vez que visitan un sitio web. A diferencia de las cookies, los usuarios desconocen que se están utilizando píxeles. De hecho, «para mitigar el uso de los píxeles de seguimiento por tu cuenta, normalmente tienes que utilizar extensiones del navegador que pueden alterar el funcionamiento del sitio web, desactivar todas las solicitudes de imágenes en un sitio o ver los correos electrónicos solo en texto sin formato»¹⁹. En otras palabras, desactivar esta tecnología de seguimiento requiere conocimientos técnicos avanzados.

Según la Agencia de Protección del Consumidor de EE. UU., los píxeles pueden monetizarse de diversas formas: la venta de publicidad dirigida, la optimización de los propios sistemas de segmentación de las plataformas, entre otras. En 2022, The Markup y STAT —medios de comunicación alternativos centrados en la tecnología y la salud, respectivamente— revisaron 100 sitios web de hospitales

¹⁷ Newman, L. H. (2022). La imagen viral de Internet que nunca has visto. En T. Bosch (Ed.), *No se espera que entiendas esto: Cómo 26 líneas de código cambiaron el mundo*. Princeton University Press. <https://www.jstor.org/stable/j.ctv2ks6t89.18>

¹⁸ Comisión Federal de Comercio, Oficina de Tecnología. (16 de marzo de 2023). *Acechando bajo la superficie: los impactos ocultos del seguimiento de píxeles*. <https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/03/lurking-beneath-surface-hidden-impacts-pixel-tracking>

¹⁹ Newman, L. H. (2022). La imagen viral de Internet que nunca has visto. En T. Bosch (Ed.), *No se espera que entiendas esto: Cómo 26 líneas de código cambiaron el mundo*. Princeton University Press. <https://www.jstor.org/stable/j.ctv2ks6t89.18>



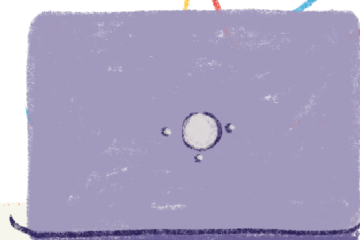
estadounidenses. En 33 de ellos, encontraron un rastreador llamado Meta Pixel que «enviaba un paquete de datos a Facebook cada vez que una persona hacía clic en un botón para concertar una cita con el médico. Los datos están vinculados a una dirección IP —un identificador que es como la dirección postal de un ordenador y que, por lo general, puede asociarse a una persona o un hogar concretos—, lo que proporciona a Facebook un registro detallado de la solicitud de cita»²⁰.

Como parte de su investigación, también examinaron sitios web utilizados para prestar servicios de telesalud y descubrieron que 13 de los 50 sitios contenían al menos un rastreador de Meta, Google, TikTok, Bing, Snap, Twitter, LinkedIn o Pinterest²¹. Estos rastreadores —en algunos casos, píxeles— recopilaban información sobre respuestas relacionadas con «autolesiones, consumo de drogas y alcohol, y [...] datos personales —incluidos nombre, dirección de correo electrónico y número de teléfono— y la enviaban a Facebook»²². Como hemos visto, estos pequeños fragmentos de código incrustados en imágenes transparentes en correos electrónicos o en páginas web tienen el potencial de recopilar datos de cualquier persona que abra el correo electrónico o visite el sitio web, y son utilizados por diversos gigantes tecnológicos.

²⁰ Feathers, T., Fondrie-Teitler, S., Waller, A. y Mattu, S. (16 de junio de 2022). *Facebook está recibiendo información médica confidencial de las páginas web de los hospitales*. The Markup. <https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites>

²¹ Feathers, T., Palmer, K. y Fondrie-Teitler, S. (13 de diciembre de 2022). *«Fuera de control»: Decenas de startups de telesalud enviaron información sanitaria confidencial a las grandes empresas tecnológicas*. The Markup. <https://themarkup.org/pixel-hunt/2022/12/13/out-of-control-dozens-of-telehealth-startups-sent-sensitive-health-information-to-big-tech-companies>

²² Feathers, T., Palmer, K. y Fondrie-Teitler, S. (13 de diciembre de 2022). *«Fuera de control»: Decenas de startups de telesalud enviaron información sanitaria confidencial a las grandes empresas tecnológicas*. The Markup. <https://themarkup.org/pixel-hunt/2022/12/13/out-of-control-dozens-of-telehealth-startups-sent-sensitive-health-information-to-big-tech-companies>



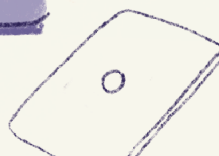
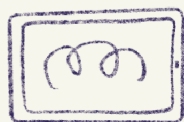
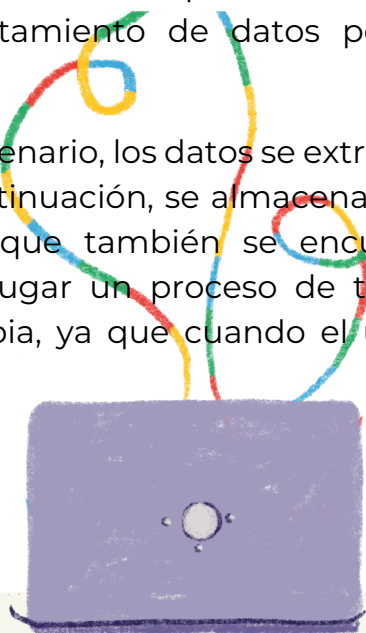
1.3. EL TRATAMIENTO DE DATOS PERSONALES A TRAVÉS DE ESTAS TECNOLOGÍAS TIENE LUGAR EN COLOMBIA Y EN OTROS PAÍSES DEL SUR GLOBAL

Tras haber explicado cómo funciona la recopilación local de datos a través de cookies, SDK y píxeles —y sabiendo que existen muchos otros métodos utilizados por los gigantes tecnológicos para tratar datos personales—, explicaremos ahora por qué se puede afirmar que este tratamiento de datos personales tiene lugar en Colombia y, por lo tanto, está sujeto a la Ley 1581 de 2012. También destacamos que este argumento es extensible a otros países en los que, sin lugar a dudas, las técnicas de recogida y tratamiento son las mismas y en los que se están tratando los datos de sus residentes.

Recordemos que las cookies son mecanismos que permiten la recogida de datos personales, el almacenamiento de información y la transmisión de dicha información. Como se ha explicado anteriormente, esto ocurre porque las cookies son pequeños archivos de texto creados y enviados por los sitios web a los dispositivos de los usuarios para obtener y almacenar información sobre ellos. Esta información es recuperada por el sitio web cuando el mismo usuario lo visita de nuevo.

Las cookies persistentes —es decir, aquellas que duran más tiempo y no caducan con cada sesión— se almacenan en el dispositivo electrónico del usuario. Si ese dispositivo se encuentra en Colombia, las operaciones de recolección, transferencia y almacenamiento de los datos personales se producen, total o inicialmente, en territorio colombiano —y lo mismo es aplicable a cualquier otro país—. En consecuencia, el tratamiento de datos personales tiene lugar en Colombia.

De hecho, en este escenario, los datos se extraen de un usuario ubicado en Colombia y, a continuación, se almacenan en una cookie instalada en su dispositivo —que también se encuentra en Colombia—. A continuación, tiene lugar un proceso de transmisión de datos que comienza en Colombia, ya que cuando el usuario regresa y visita el

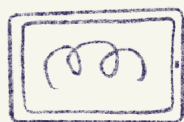
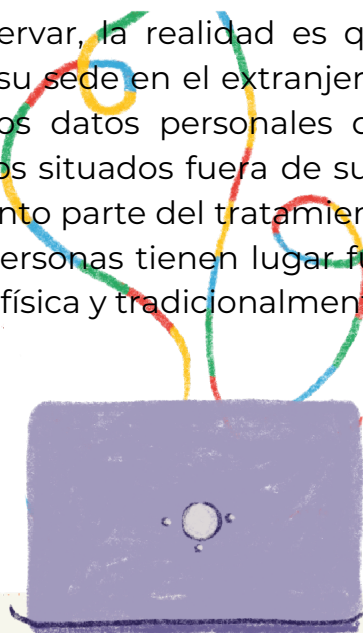


mismo sitio web, la cookie se transfiere desde el dispositivo ubicado en Colombia al servidor del sitio web, que pretende leer la información. Así pues, aunque el servidor que recibe los datos se encontrara en otro país, dicha recogida de datos tuvo lugar inicialmente en Colombia, ya que el dispositivo se encuentra dentro de nuestro territorio. Por consiguiente, es en Colombia donde se instaló la cookie y donde se capturaron los datos que permiten identificar al usuario en futuras visitas.

Una situación similar se da en el caso de los SDK. Como se ha descrito anteriormente, los SDK son componentes básicos y necesarios para el funcionamiento de las aplicaciones tecnológicas. Estas aplicaciones, a su vez, están disponibles para su descarga en plataformas como Google Play Store o Apple App Store. Una vez que las aplicaciones se encuentran en dispositivos móviles situados en territorio colombiano, ejecutan sus propios SDK y los de terceros, lo que facilita la recogida de datos de los usuarios de las aplicaciones. Esta recogida tiene lugar en Colombia —o en el país en que se encuentre el usuario—, en la medida en que las aplicaciones y sus SDK operativos estén instalados en dispositivos móviles situados en nuestro territorio. Por lo tanto, la recogida se produce en territorio colombiano.

Por último, nos gustaría destacar que, si bien los píxeles no se descargan en el dispositivo, se trata de imágenes transparentes que —aunque invisibles para el ojo humano— se muestran en las pantallas de los dispositivos de los usuarios. Una vez que la orden de recogida de datos entra en vigor, esta puede enviarse desde un servidor en el extranjero, pero la recogida propiamente dicha tiene lugar en el dispositivo ubicado en Colombia. Así pues, parte del tratamiento se lleva a cabo en nuestro país.

Como se puede observar, la realidad es que, aunque las empresas tecnológicas tengan su sede en el extranjero y presten sus servicios a través de Internet, los datos personales que tratan se extraen de personas y dispositivos situados fuera de sus territorios. Esto significa que, en la práctica, tanto parte del tratamiento como el impacto sobre los derechos de las personas tienen lugar fuera de la jurisdicción a la que están vinculadas física y tradicionalmente.

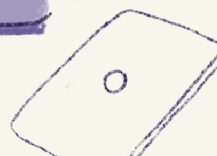
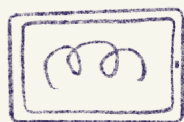
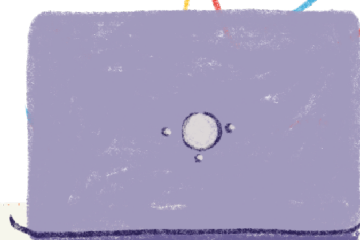


Una interpretación tradicional y anacrónica de la territorialidad ha llevado a las grandes empresas tecnológicas a resistirse a cumplir con las leyes de protección de datos de los países en los que tratan datos y de los que extraen datos personales que monetizan. Esto ha ocurrido principalmente en países del Sur Global, que carecen de un capital político ni remotamente comparable al de la Unión Europea, la cual ha logrado hacer cumplir con éxito su normativa en materia de protección de datos personales.

En Colombia, por ejemplo, la Oficina de Protección de Datos Personales de la Superintendencia de Industria y Comercio (SIC) ha realizado un esfuerzo significativo para garantizar la protección de los datos personales de los colombianos. La SIC ha basado su competencia y la aplicación de la legislación colombiana precisamente en el hecho de que el tratamiento de datos personales tiene lugar en Colombia, y ha dictado resoluciones que obligan a las grandes empresas a cumplir con los requisitos legales para dicho tratamiento.

Sin embargo, al menos tres de estas grandes empresas tecnológicas han interpuesto demandas²³ con el fin de impugnar la competencia de la SIC y negarse a cumplir la legislación colombiana. Entre los argumentos esgrimidos por estas empresas, destacan que, en su opinión, el tratamiento de datos personales no tiene lugar en territorio colombiano, sino en servidores ubicados en el extranjero; que, a falta de un tratado internacional, bilateral o multilateral que faculte a la autoridad colombiana de protección de datos para conocer de sus

²³ **Asunto «Google LTDA»**, n.º de expediente: 25000234100020220044800, Asunto: Anulación y restablecimiento con suspensión provisional de las Resoluciones 70315, de 4 de noviembre de 2020, y 38869, de 24 de junio de 2021; Presentada el 21 de abril de 2022; Juez presidente: LUIS NORBERTO CERMEÑO; Demandante: GOOGLE COLOMBIA LTDA, Demandada: SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO; **Caso Google LLC**, N.º de expediente: 25000234100020220044400, Objeto: nulidad y restablecimiento de derechos con suspensión provisional de las resoluciones n.º 53593, de 3 de septiembre de 2020, n.º 14010, de 16 de marzo de 2021, y n.º 60478, de 21 de septiembre de 2021, Presentada el 20 de abril de 2022, Jueza ponente: ANA MARGOTH CHAMORRO BENAVIDES, Demandante: GOOGLE LLC, Demandada: SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO; **Caso WhatsApp**, demandante: WhatsApp LLC, demandada: SIC, n.º de expediente: 25000-23-41-000-2022-01520-00, Asunto: Anulación y restablecimiento de derechos en relación con las Resoluciones 4554 de 2022, 29826 de 2021 y 15342 de 2022, Jueza: Ana Margoth Chamorro Benavides, Fecha de la demanda: 06/12/2022; **Caso TikTok**, demandante: ByteDance LTD, demandado: SIC, n.º de expediente: 25000234100020220106400, Asunto: Anulación y restablecimiento de derechos — Resoluciones 62132, de 5 de octubre de 2020, 14015, de 16 de marzo de 2021, y 75009, de 22 de noviembre de 2021, dictadas por la SIC.



casos, cualquier medida adoptada por esta resulta irregular; y que tienen su domicilio social en otros países y no cuentan con oficinas en el territorio nacional. No obstante, en la mayoría de los casos, estas empresas son accionistas mayoritarias y ejercen el control sobre sociedades constituidas con arreglo a la legislación colombiana, aunque sostengan que son entidades jurídicas independientes.

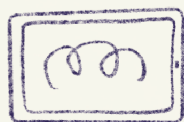
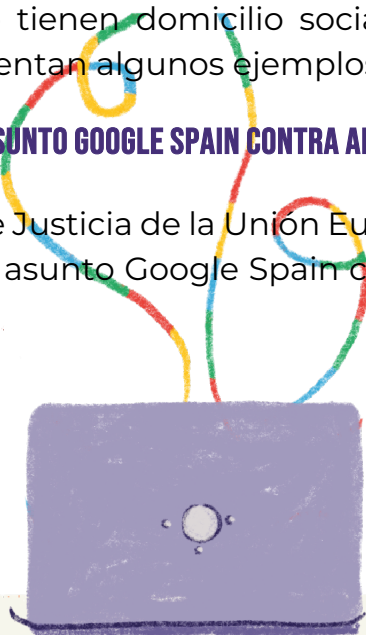
En última instancia, esto pone de relieve la falta de protección a la que se enfrentan millones de personas que utilizan a diario servicios digitales en países distintos de aquellos en los que tienen su sede las grandes empresas que los prestan. Estas personas quedan indefensas ante el inmenso poder económico y político de las grandes empresas tecnológicas, que acaban extrayendo sus datos y convirtiéndolos en un importante activo económico. A continuación, estos datos se utilizan para personalizar contenidos y, en ocasiones, para manipular las mentes, influyendo no solo en las decisiones de los consumidores, sino también en las preferencias políticas y en otros ámbitos. En las secciones siguientes, profundizamos en algunas de estas dimensiones y en cómo se han materializado estos riesgos en diversos países de la región.

1.4. LAS PRINCIPALES PLATAFORMAS HAN TENIDO QUE RENDIR CUENTAS ANTE OTRAS JURISDICCIONES

El tratamiento de datos personales en distintos territorios plantea un reto a la hora de evaluarlo y de garantizar la protección jurídica de los interesados. En este contexto, diversos tribunales de todo el mundo han reconocido que las empresas con sede en el extranjero no pueden eludir la aplicación de las leyes locales de protección de datos alegando formalmente que no tienen domicilio social en un país concreto. A continuación, se presentan algunos ejemplos:

1.4.1. EL ASUNTO GOOGLE SPAIN CONTRA AEPD (2014)

En 2014, el Tribunal de Justicia de la Unión Europea (TJUE) se pronunció sobre el mencionado asunto Google Spain contra la Agencia Española



de Protección de Datos (C-131/12)²⁴ . El asunto se originó a raíz de una solicitud de un ciudadano español para que Google eliminara de sus resultados de búsqueda un enlace que dañaba su reputación. Google alegó que la normativa europea en materia de protección de datos no le era aplicable, ya que su sede central se encontraba en Estados Unidos y el tratamiento de datos se realizaba fuera del territorio europeo.

El Tribunal rechazó este argumento y concluyó que Google estaba sujeta a la legislación europea, ya que existía un vínculo directo entre las actividades de la empresa matriz estadounidense y las de su filial en España. En opinión del Tribunal,

«Google Inc. gestiona Google Search desde un punto de vista técnico y administrativo, y no se ha demostrado que Google España lleve a cabo en España ninguna actividad directamente vinculada a la indexación o el almacenamiento de información o datos contenidos en sitios web de terceros. Sin embargo, la promoción y venta de espacios publicitarios —de las que Google España es responsable en España— constituye la parte esencial de la actividad comercial del grupo Google y puede considerarse estrechamente vinculada a Google Search».²⁵ (negrita añadida).

Así pues, el TJUE interpretó el concepto de «establecimiento» de manera amplia y estableció una norma para la aplicación funcional de la ley: cuando una empresa opera en un territorio a través de filiales que permiten o hacen rentable su actividad económica, está obligada a cumplir la normativa de protección de datos de ese país.

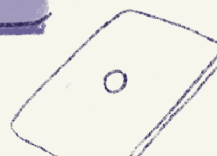
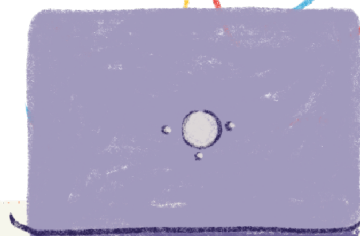
1.4.2. EL ASUNTO GOOGLE CONTRA CNIL (2019)

Otro precedente significativo fue el asunto Google LLC contra CNIL, resuelto en 2019 por el TJUE²⁶ y posteriormente por el Consejo de Estado francés. La autoridad francesa de protección de datos (CNIL) impuso una multa a Google por negarse a desindexar a nivel mundial los

²⁴ TJUE. Google Spain contra AEPD (C-131/12, 2014). En: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:62012CJ0131>

²⁵ Ibid.

²⁶ TJUE. Google contra CNIL (C-507/17, 2019). Disponible en: [https://eur-lex.europa-eu.translate.google/legal-content/EN/TXT/?uri=celex:62017CJ0507&x_tr_sl=en&x_tr_tl=es&x_tr_hl=es&x_tr_pto=tc](https://eur-lex.europa.eu.translate.google/legal-content/EN/TXT/?uri=celex:62017CJ0507&x_tr_sl=en&x_tr_tl=es&x_tr_hl=es&x_tr_pto=tc)



resultados de búsqueda solicitados en virtud del «derecho al olvido». Google argumentó que su obligación debía limitarse a los dominios europeos de su motor de búsqueda y no debía extenderse al resto del mundo.

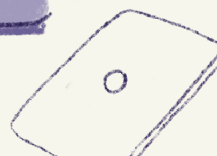
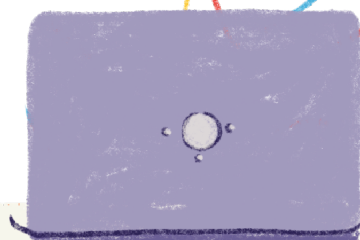
El Tribunal de Justicia de la Unión Europea reconoció que la protección del derecho al olvido debe sopesarse con la libertad de información, pero dejó claro que las autoridades nacionales pueden exigir la aplicación extraterritorial de las normas cuando sea necesario para garantizar la eficacia de los derechos de las personas. Esta sentencia se hace eco del razonamiento del caso español, en el sentido de que

«[E]l establecimiento de Google en territorio francés lleva a cabo, entre otras cosas, actividades comerciales y publicitarias que están indisolublemente vinculadas al tratamiento de datos personales para el funcionamiento del motor de búsqueda en cuestión; y, en segundo lugar, que dicho motor de búsqueda — dada, entre otras cosas, la existencia de pasarelas entre sus distintas versiones nacionales— debe considerarse que lleva a cabo un único tratamiento de datos personales. El tribunal remitente considera que, en estas circunstancias, dicho tratamiento se lleva a cabo en el marco del establecimiento de Google en Francia» (énfasis añadido)

En su resolución definitiva, el Consejo de Estado francés confirmó la sanción impuesta por la CNIL y subrayó que las empresas globales deben garantizar el cumplimiento coherente de las decisiones en materia de protección de datos en todas las versiones territoriales de sus servicios.

1.4.3. LOS ASUNTOS SCHREMS I (2015) Y SCHREMS II (2020)

Tras el asunto Google Spain, el TJUE amplió su jurisprudencia sobre la dimensión transfronteriza del «habeas data». En los asuntos Schrems I (C-362/14) y Schrems II (C-311/18), el Tribunal examinó la legalidad de los mecanismos que permiten la transferencia de datos personales desde la Unión Europea a Estados Unidos. En el primer caso, conocido como Schrems I, el Tribunal declaró nulo el acuerdo «Safe Harbor», al



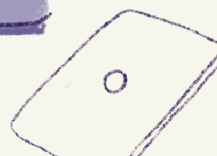
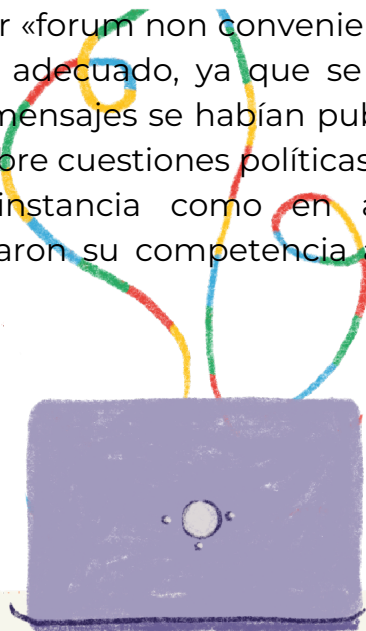
considerar que el sistema estadounidense no garantizaba un nivel adecuado de protección frente a la vigilancia masiva por parte de los servicios de inteligencia.

El demandante, Max Schrems, demostró que los organismos de seguridad estadounidenses podían acceder a los datos personales transferidos desde Europa a Estados Unidos sin una supervisión judicial efectiva, lo que violaba los principios de proporcionalidad y necesidad en el tratamiento de datos. El TJUE concluyó que las empresas europeas —o aquellas que operan en Europa— no podían trasladar sus responsabilidades a las autoridades de otro país y que la protección debía garantizarse en todo momento, independientemente del lugar en el que se almacenaran los datos.

En el caso Schrems II, el Tribunal llegó a una conclusión aún más contundente: invalidó el mecanismo del «Privacy Shield» —sucesor del «Safe Harbor»— reiterando que la protección de los datos personales es un derecho fundamental que no puede verse menoscabado por acuerdos comerciales ni por mecanismos de autorregulación. En dicha sentencia, el TJUE sostuvo que las empresas que transfieren datos fuera de la Unión Europea deben garantizar que las personas disfruten de un nivel de protección sustancialmente equivalente al que ofrece la legislación de la UE.

1.4.4. EL CASO DE TWITTER EN CANADÁ: GIUSTRA CONTRA TWITTER, INC. (2021)

Este caso se presentó ante los tribunales de Columbia Británica (Canadá) después de que el Sr. Giustra interpusiera una demanda por unos tuits que, en su opinión, dañaban su reputación. Twitter, la parte demandada en el proceso, solicitó que se desestimara el caso por falta de competencia o por «forum non conveniens». En opinión de Twitter, California era el foro adecuado, ya que se trataba de una empresa estadounidense, los mensajes se habían publicado principalmente en EE. UU. y versaban sobre cuestiones políticas de ese país. Sin embargo, tanto en primera instancia como en apelación, los tribunales canadienses confirmaron su competencia alegando que los tuits se



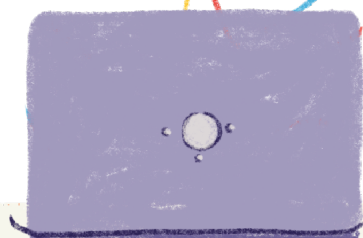
habían publicado en Columbia Británica y habían causado un perjuicio a un residente de Columbia Británica²⁷.

1.4.5. EL CASO CONTRA MICROSOFT RESUELTO POR EL TRIBUNAL SUPERIOR DE JUSTICIA DE BRASIL (2020)

Un directivo de una empresa de transportes de Brasil que recibió amenazas desde una cuenta de correo de Microsoft promovió una acción contra Microsoft solicitando que ésta le suministrara los registros de acceso (IP, fecha y hora) que permitieran identificar al autor de las amenazas. El juzgado de primera instancia concedió la tutela anticipada y fijó una multa diaria de R\$ 10.000 por incumplimiento; ante la negativa de la empresa a entregar los datos, la multa se ejecutó provisoriamente hasta alcanzar R\$ 310.000. Microsoft, en su defensa, sostuvo que la justicia brasileña era incompetente porque las amenazas estaban escritas en inglés, la cuenta de correo había sido accedida desde el extranjero, el proveedor de conexión también estaba fuera de Brasil, y que cumplir la orden implicaría violar la legislación de los Estados Unidos, lugar donde se habría producido el acceso. No obstante, el Tribunal Superior de Justicia de Brasil, rechazó el argumento por unanimidad, y resaltó que basta con que al menos un dispositivo (el del usuario amenazado, en este caso) implicado en el tratamiento de datos personales se encuentre en territorio nacional para que se aplique la legislación nacional, al margen de si se trata de una empresa extranjera:

«Es un equívoco imaginar que cualquier aplicación alojada fuera de Brasil no pueda ser alcanzada por la jurisdicción nacional o que las leyes brasileñas no sean aplicables a sus actividades. Se aplica la ley brasileña siempre que cualquier operación de recolección, almacenamiento, guarda y tratamiento de registros, de datos personales o de comunicaciones por proveedores de conexión y de aplicaciones de internet ocurra en territorio nacional,

²⁷ Véase Bookman, P. K. (2024). «If Not Here, Where?: Transnational Litigation Against U.S. Tech Giants Around the World». 56 New York University Journal of International Law and Politics 29. Disponible en Faculty Scholarship, Facultad de Derecho de Fordham (https://ir.lawnet.fordham.edu/faculty_scholarship/1337)



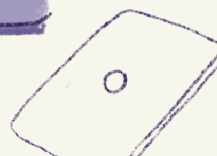
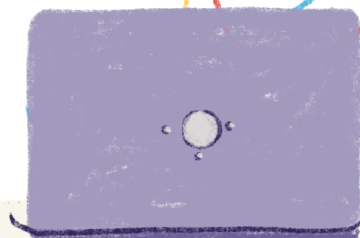
aunque solo uno de los dispositivos de la comunicación esté en Brasil y aunque las actividades sean realizadas por empresa con sede en el extranjero." (traducción propia, sumario, puntos 5 y 6)».

«La recurrente, por sí sola, es empresa subsidiaria destinada exclusivamente a operaciones en Brasil, pero pertenece al grupo económico de reconocimiento mundial.» (traducción propia, par. XXXI de la relatora Adigri)

1.4.6. EL CASO P.A.E. CONTRA FACEBOOK ARGENTINA S.R.L. (MEDIDA AUTOSATISFACTIVA DE 2019)

En este caso, una persona interpuso una medida autosatisfactiva contra Facebook Argentina SRL para solicitar que se eliminaran publicaciones que contenían el nombre e imagen de sus hijos. El Juez de instancia otorgó la medida inicialmente. Sin embargo, esa decisión fue apelada por Facebook Argentina argumentando falta de legitimidad pasiva, dado que no es ella quien opera el sitio web "facebook.com". El Tribunal Superior confirmó el pronunciamiento del juez de instancia y señaló que la excepción de falta de legitimidad era improcedente, dado que la filial se encuentra bajo la aplicación de la legislación argentina. La sentencia resalta que, más allá de las formas societarias que la empresa adopte, se encuentra representada en el país; y que, además, la constitución societaria en el extranjero no significa que no le sean de aplicación las normas del país, cuando los actos y contratos se celebran en el mismo:

«La sociedad constituida en el extranjero se rige, en cuanto a su existencia y forma por las leyes del lugar de constitución, lo que no obsta para aplicar las leyes argentinas a los actos y contratos que se celebren en nuestro país, pues su radicación en éste importa un total sometimiento a la jurisdicción y leyes argentinas, aunque su capacidad se rija por la ley de domicilio. Tampoco escapa al análisis el hecho de que las redes sociales, así como otras formas de comunicaciones electrónicas y tratamientos de datos a través de Internet, han constituido un marco complejo de competencias jurisdiccionales y responsabilidades que requieren



de una legislación adecuada y específica. Sin embargo, esa situación no es impedimento para que los jueces puedan responder ante el planteo de un caso concreto. (...)

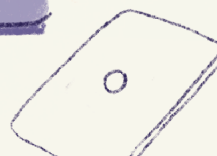
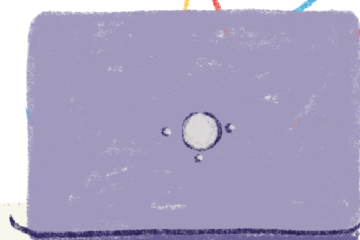
Facebook Argentina S.R.L. no puede eludir las mandas judiciales impuestas alegando que carece de facultades para ello, por lo que la firma debe hacer conocer y cumplir las resoluciones judiciales notificadas al domicilio por ella constituida en el país».

1.5. EL CASO DE LA TRIBUTACIÓN

En esta sección nos hemos centrado tanto en los riesgos como en la falta de fundamento jurídico que subyace a la reticencia de las grandes empresas tecnológicas a reconocer la jurisdicción de otros países sobre ellas, y especialmente en las implicaciones que esto tiene para garantizar el derecho a la protección de los datos personales. Sin embargo, lo cierto es que esta reticencia también existe en otros ámbitos jurídicos y repercute en otros derechos. A continuación, analizaremos otro ejemplo.

La creciente digitalización de la economía ha puesto de manifiesto las limitaciones del sistema tributario internacional tradicional, que fue diseñado para empresas que operaban mediante una presencia física en un territorio determinado. Hoy en día, las grandes plataformas y los proveedores de servicios digitales pueden generar ingresos significativos procedentes de usuarios y consumidores ubicados en países como Colombia sin necesidad de establecer una presencia física allí, lo que reduce la capacidad de estos Estados para gravar los ingresos generados en sus mercados. Este fenómeno ha sido identificado por el proyecto BEPS de la OCDE²⁸ como uno de los principales retos de la fiscalidad internacional: mientras que las principales economías — donde se encuentran las sedes de las empresas digitales— acaparan

²⁸ Los pilares I y II forman parte del proyecto para combatir la erosión de la base imponible y el desplazamiento de beneficios (BEPS) liderado por la OCDE y el G-20. El pilar I tiene por objeto reasignar parcialmente los derechos de tributación a los países en los que se encuentran los usuarios o los mercados, incluso en ausencia de una presencia física, especialmente en el caso de las grandes empresas multinacionales. El pilar II, por su parte, establece un impuesto mínimo global —generalmente del 15 %— para garantizar un nivel mínimo de tributación efectiva y reducir los incentivos para trasladar los beneficios a jurisdicciones con impuestos bajos o nulos (OCDE, 2021).

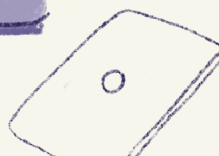
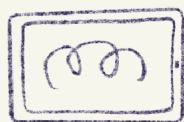


una mayor parte de los ingresos fiscales, los países donde se encuentran los usuarios y consumidores reciben una parte mucho menor de esos recursos.

Esto contribuye a agravar las desigualdades globales, ya que reduce la capacidad de los países de bajos ingresos para financiar políticas públicas y garantizar los derechos fundamentales a sus poblaciones. Los ingresos que los gobiernos pueden recaudar constituyen la principal fuente de financiación para garantizar derechos como la asistencia sanitaria, la educación, la protección social y el acceso a la justicia. Cuando las normas internacionales impiden que los países en los que se generan el consumo y el valor económico graven adecuadamente los ingresos derivados de los servicios digitales, su capacidad fiscal se ve mermada, lo que limita su capacidad para invertir en los sectores sociales.

En este sentido, es fundamental tratar de reforzar la tributación de los servicios digitales transfronterizos, de modo que los países en los que se generan el consumo y el valor económico puedan participar de forma más equitativa en la recaudación de ingresos fiscales. Para ello, deben promoverse mecanismos que permitan gravar estas actividades más allá de la presencia física de las empresas, y deben apoyarse iniciativas internacionales como la Convención Marco de las Naciones Unidas sobre Cooperación Fiscal Internacional²⁹ —destinada a una distribución más equitativa de los derechos de tributación en la economía digital—.

²⁹ Véase: <https://financing.desa.un.org/unfcitc>



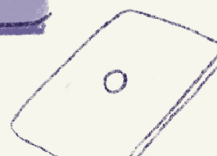
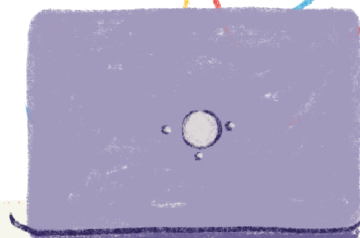
1.6. CONCLUSIÓN: LAS EMPRESAS TECNOLÓGICAS ESTÁN VIOLANDO LOS DERECHOS A LA PROTECCIÓN DE LOS DATOS PERSONALES Y OTROS DERECHOS FUNDAMENTALES DE MILLONES DE PERSONAS QUE VIVEN EN PAÍSES COMO COLOMBIA AL NEGARSE A CUMPLIR CON LA NORMATIVA NACIONAL Y A RECONOCER LA JURISDICCIÓN DE SUS AUTORIDADES.

El hecho de no reconocer la jurisdicción y la autoridad de gobiernos como el de Colombia, así como la renuencia de las grandes empresas de tecnología digital a cumplir con las leyes de los países en los que no tienen su sede, está provocando graves violaciones de los derechos humanos. En esta sección, nos centramos principalmente en el derecho de hábeas data, ya que creemos que los datos personales son el motor del modelo de negocio de las grandes empresas tecnológicas y constituyen su activo más importante. También nos centramos en este derecho concreto porque su vulneración amenaza «otros derechos que pueden verse afectados debido a la disponibilidad masiva de datos personales en manos de terceros y a la mayor potencia computacional que esto otorga a quienes los tratan»³⁰. De hecho, como se analizará más adelante, ciertos grupos de población son especialmente vulnerables al uso de sus datos, y valores esenciales como la democracia corren peligro debido al uso manipulador de los datos personales. Del mismo modo, derechos como la salud física y mental se ven afectados por el diseño adictivo, la elaboración de perfiles y la influencia en los hábitos de consumo.

En la medida en que las interacciones actuales tienen lugar principalmente —aunque no de forma exclusiva— en el ciberespacio³¹ y a través de Internet, es esencial reforzar la autoridad y la jurisdicción de las autoridades locales para proteger los derechos de sus ciudadanos. Esta es la opinión de la Corte Constitucional de Colombia, que ha

³⁰ Ángel, M. P. (2025). Minería de datos: la inteligencia artificial y sus implicaciones para la privacidad y la protección de datos personales en Colombia. En H. Rank (Ed.), Cinco perspectivas sobre el presente y el futuro de la inteligencia artificial en Colombia (pp. 50-65). Konrad-Adenauer-Stiftung

³¹ Definido por el MinTic como «el entorno físico y virtual compuesto por ordenadores, sistemas informáticos, programas informáticos (software), redes de telecomunicaciones, datos e información que se utiliza para la interacción entre los usuarios». <https://www.mintic.gov.co/portal/inicio/Glosario/>



insistido en que «el Estado no puede renunciar a su jurisdicción sobre Internet»³² ; por lo tanto, en este caso, el principio de territorialidad se utiliza «para determinar si la controversia tiene una conexión relevante con el país, como la prestación de servicios a usuarios en Colombia o el tratamiento de datos personales dentro del territorio nacional»³³ . La Corte también ha señalado que, «cuando se produzca una amenaza o una violación de los derechos fundamentales en el ciberespacio, el juez que conozca del recurso de tutela tendrá competencia para pronunciarse sobre si dicha amenaza o violación tiene efectos relevantes en Colombia»³⁴ .

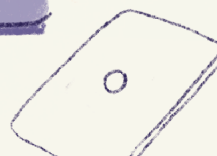
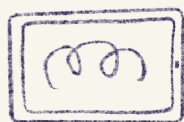
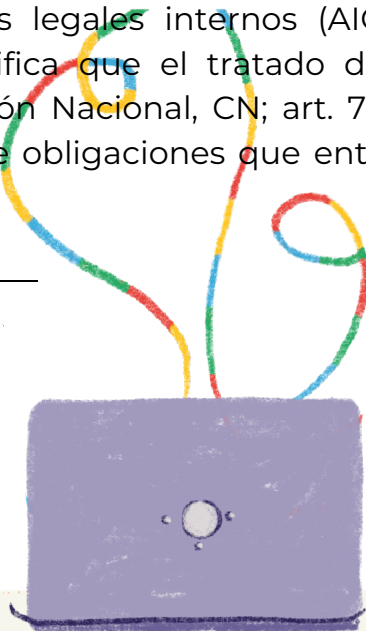
2. DEBILITAMIENTO DE LAS NORMAS DE PROTECCIÓN DE DATOS PERSONALES RECOPIADOS POR LAS PLATAFORMAS Y SU TRANSFERENCIA A LOS ESTADOS UNIDOS EN VIRTUD DE ACUERDOS BILATERALES

El Acuerdo entre los Estados Unidos de América y la República Argentina sobre Inversión y Comercio Recíproco («AICR»), firmado en febrero de 2026, liberaliza el comercio entre ambos países mediante la eliminación por parte de la República Argentina de las barreras arancelarias y no arancelarias a los productos estadounidenses, la reducción de las subvenciones y los privilegios comerciales para las empresas estatales argentinas, la armonización de las normas nacionales de calidad para permitir la entrada de mercancías procedentes de Estados Unidos, la reforma del régimen de propiedad intelectual, la apertura del mercado minero (AICR; anexo III, art. 4) y la eliminación de determinadas protecciones de los datos personales (AICR; anexo III, art. 2). El AICR entrará en vigor sesenta días después de la fecha en que ambos Estados certifiquen el cumplimiento de sus respectivos requisitos legales internos (AICR; 6.7). En la República Argentina, esto significa que el tratado debe ser aprobado por el Congreso (Constitución Nacional, CN; art. 75, apartado 22), ya que el instrumento contiene obligaciones que entran dentro del ámbito de

³² Ibid.

³³ Ibid.

³⁴ Ibid.



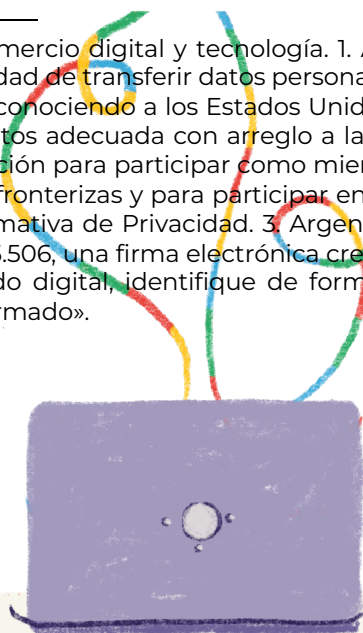
competencia del poder legislativo y que exceden el alcance de la autoridad del poder ejecutivo.

El artículo 2 del anexo III del AICR, que detalla los compromisos asumidos por Argentina en virtud del tratado, contiene una serie de modificaciones significativas del marco jurídico nacional en materia de datos personales.

El AICR tiene por objeto «proporcionar seguridad jurídica» para la exportación a los Estados Unidos de datos personales recopilados en la República Argentina. A este respecto, el AICR establece que, a efectos de la transferencia de datos personales a los Estados Unidos, Argentina considerará que los Estados Unidos garantizan una protección jurídica «adecuada» para dichos datos³⁵. Además, el AICR prevé la participación de la República Argentina en foros multilaterales a través de los cuales se promueva el flujo transfronterizo de datos y la cooperación internacional entre las autoridades de control en materia de tratamiento de datos. Por último, la AICR establece que los documentos firmados electrónicamente en los Estados Unidos deben considerarse equivalentes a los documentos firmados digitalmente, produciendo los mismos efectos jurídicos que una firma digital y cumpliendo los requisitos de integridad y autenticidad establecidos en la legislación nacional (Ley 25 506; artículos 5, 7, 8, 9 y 11).

El artículo 12 de la Ley 25 326 prohíbe la transferencia de datos personales de cualquier tipo a «países u organizaciones internacionales o supranacionales que no ofrezcan niveles adecuados de protección». La Agencia de Acceso a la Información Pública (AAIP) determina, bien por iniciativa propia o a petición de una parte, qué países u

³⁵ AICR, Anexo III, art. 2 («Comercio digital y tecnología. 1. Argentina garantizará la seguridad jurídica respecto a la posibilidad de transferir datos personales desde su territorio a los Estados Unidos, entre otras cosas, reconociendo a los Estados Unidos como un país o jurisdicción que ofrece una protección de datos adecuada con arreglo a la legislación argentina. 2. Argentina presentará su carta de intención para participar como miembro asociado en el Foro Global de Normas de Privacidad Transfronterizas y para participar en el Acuerdo de Cooperación Global para la Aplicación de la Normativa de Privacidad. 3. Argentina reconocerá como firma digital válida, con arreglo a la Ley 25.506, una firma electrónica creada en los Estados Unidos que esté respaldada por un certificado digital, identifique de forma fiable al firmante y garantice la integridad del documento firmado»).



organizaciones ofrecen una protección jurídica adecuada (Decreto 1558/2001; anexo I, 12).

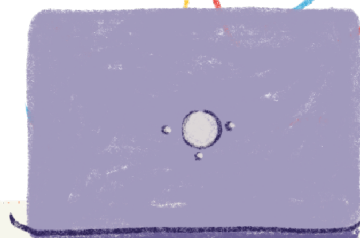
Estados Unidos nunca ha figurado ni figura actualmente en la lista de países que, según la AAIP, ofrecen una protección jurídica adecuada de los datos personales. Los factores que, a juicio de la autoridad reguladora argentina, suscitan preocupación son:

- A diferencia de la República Argentina, Estados Unidos carece de una normativa federal uniforme sobre el tratamiento de datos personales y de una autoridad de control eficaz.
- En consecuencia, las normas de «autorregulación» no son exigibles ni uniformes en los cincuenta estados de la Unión.

El AICR constituiría una excepción a la prohibición de las transferencias de datos personales, ya sea como «tratado internacional del que Argentina es parte» (tal y como se establece en el artículo 12 de la Ley 25.326) o porque la AAIP emita —ya sea por instrucción del presidente o mediante el cumplimiento voluntario del acuerdo— una resolución en la que se declare que Estados Unidos es una jurisdicción adecuada. Esto implica autorizar transferencias internacionales de datos a un país que, hasta ahora, no era considerado una «jurisdicción adecuada» por el Gobierno argentino, sin que las circunstancias en dicho país hayan cambiado en lo más mínimo; o, lo que es peor aún, a pesar de que esas circunstancias han empeorado en el contexto del uso estratégico de los datos por parte del Gobierno de EE. UU. como herramienta de vigilancia³⁶.

En virtud del AICR, la venta de datos personales a responsables o encargados del tratamiento estadounidenses —incluidas las grandes

³⁶ Esto guarda relación con el debate actual en el Congreso de los Estados Unidos sobre la renovación de la sección 702 de la Ley de Vigilancia de Inteligencia Extranjera (FISA). La sección 702 permite a las agencias de inteligencia estadounidenses recopilar datos sobre cualquier persona no estadounidense respecto de la cual exista una sospecha razonable de que se encuentra fuera del país, con el fin de obtener «información de inteligencia extranjera». Esta autorización expira en junio. El programa constituyó la base de la sentencia europea citada a continuación (Schrems II), que bloqueó las transferencias de datos entre la UE y EE. UU. Desde entonces, la Administración Biden ha impulsado ciertos cambios mediante un decreto ejecutivo, y la Unión Europea ha vuelto a permitir dichas transferencias; sin embargo, estas reformas no se han incorporado a la legislación y, bajo el mandato de Trump, persisten riesgos significativos de que la recopilación masiva de datos continúe sin las garantías adecuadas.



empresas tecnológicas con sede en ese país— ya no estará sujeta a la normativa de la ley de protección de datos ni a la AAIP, ni se exigirá el cumplimiento de las cláusulas modelo de protección ni del requisito de autorización administrativa previa en caso de que contengan disposiciones diferentes. Por el mero hecho de que sus datos se hayan vendido a Estados Unidos, los interesados ya no gozarán de las protecciones que ofrece la legislación argentina y podrían verse privados de la protección de sus tribunales.

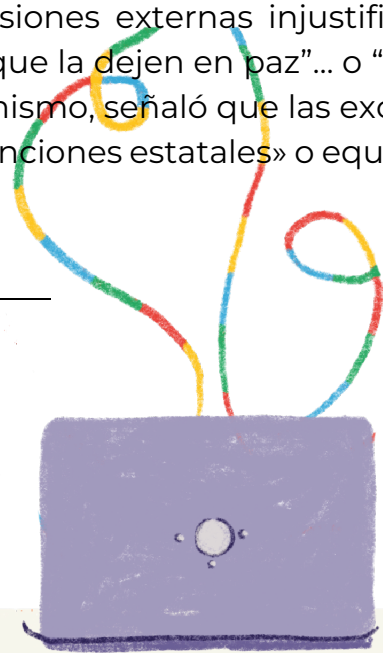
En una sentencia reciente sobre el caso «Torres Abad», el Tribunal Supremo de Justicia de la Nación interpretó el alcance de los artículos 19 y 43 de la Constitución Nacional de una manera que entra en conflicto con las disposiciones de la AICR. En dicho caso, el Tribunal declaró inconstitucional la cesión de datos personales sin el consentimiento específico de los interesados en aquellos casos en que la ley de protección de datos personales autorizaba dichas cesiones «en el cumplimiento de funciones estatales» o en virtud de un mandato legal relativo a dichas autoridades, o mediante acuerdos celebrados entre ellas en el ámbito de sus respectivas competencias.

El Tribunal sostuvo que los artículos 19 y 43, apartado 3, de la Constitución Nacional consagran el derecho a la autodeterminación informativa³⁷ —ya reconocido por la Corte Interamericana de Derechos Humanos en el caso CAJAR— y el derecho a «que se le deje en paz». En cuanto al primero, el Tribunal afirmó que «toda persona tiene la facultad de disponer de los datos que le conciernen, de decidir con quién y en qué medida desea compartirlos y, en su caso, de controlar el uso que terceros hagan de ellos».³⁸ Además, la Corte Suprema reconoció «el derecho de toda persona a disfrutar de su soledad y tranquilidad, sin ser molestada por intrusiones externas injustificadas, también conocido como el “derecho a que la dejen en paz”... o “derecho a que la dejen en tranquilidad”».³⁹ Asimismo, señaló que las excepciones legales relativas al «desempeño de funciones estatales» o equivalentes eran tan amplias

³⁷ Torres Abad, consid. 8.

³⁸ Torres Abad, consid. 8.

³⁹ Torres Abad, consid. 8.



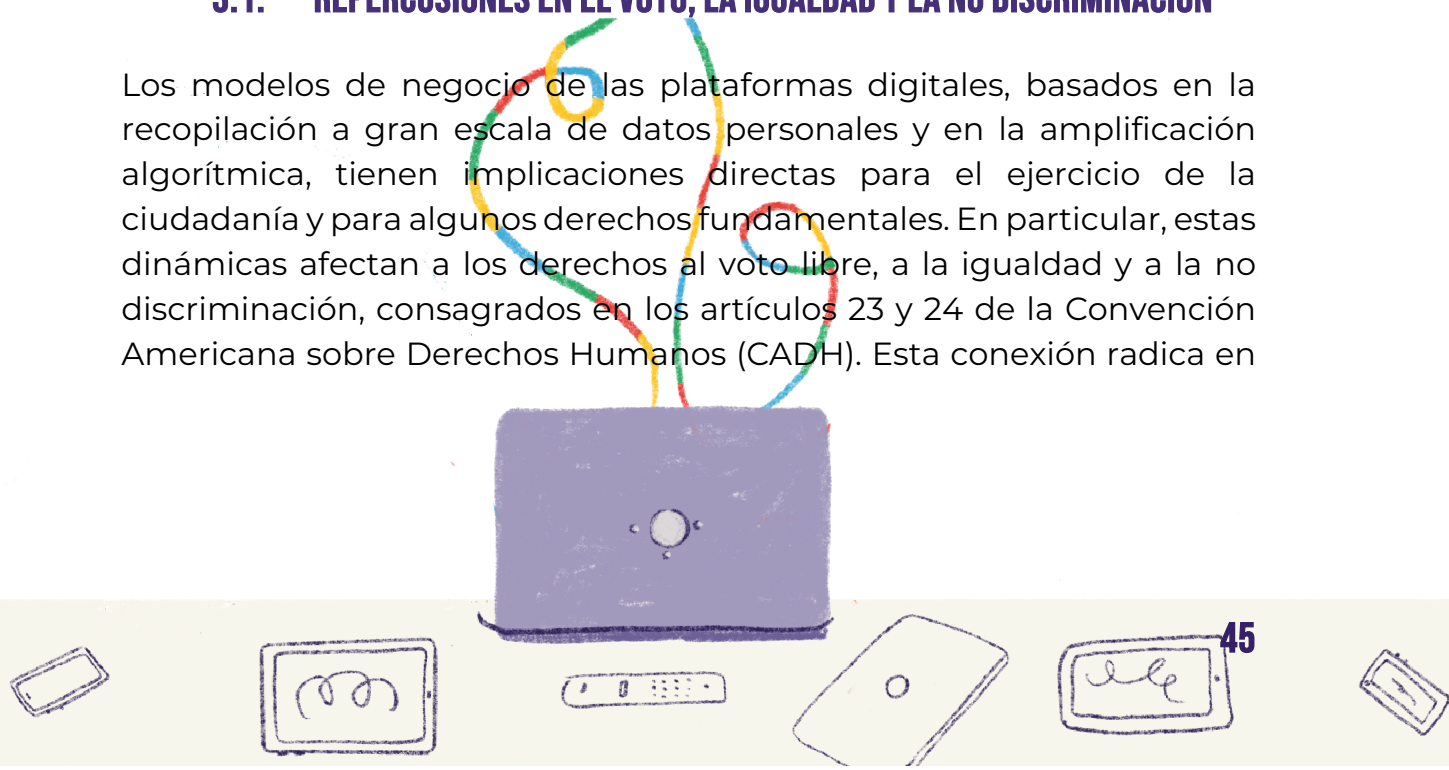
que, por sí solas, no satisfacían los requisitos de finalidad legítima o proporcionalidad.

La AICR no garantizará la autonomía informativa tal y como la reconocen la Corte Interamericana y el Tribunal Supremo, al menos en lo que respecta a las operaciones posteriores llevadas a cabo en Estados Unidos con datos personales exportados desde Argentina. Contrariamente a la posición defendida en Europa —e incluso durante décadas por las propias autoridades argentinas— de que Estados Unidos plantea riesgos generales derivados de la falta de protección jurídica y de la extensión de la jurisdicción, así como riesgos específicos derivados de la aplicación de la Ley FISA, que autoriza al Gobierno de Estados Unidos a recabar datos personales vendidos por empresas privadas con fines de vigilancia estatal, la AICR clasifica a Estados Unidos como una «jurisdicción adecuada». Como consecuencia de esta clasificación, las transferencias de datos a Estados Unidos dejarán de estar sujetas a las garantías establecidas por la Ley de Protección de Datos Personales, las cláusulas modelo o las facultades de supervisión de la AAIP una vez completada la transferencia. En consecuencia, los interesados verán reducida, si no eliminada, su capacidad para invocar el principio de consentimiento —o para impugnar la ilegalidad, la ilegitimidad o el carácter desproporcionado de los usos que puedan hacerse de sus datos— una vez que sus datos se transfieran a empresas estadounidenses y/o de estas al Gobierno federal de los Estados Unidos.

3. IMPACTOS DE LOS MODELOS DE NEGOCIO BASADOS EN DATOS EN LOS DERECHOS FUNDAMENTALES Y HUMANOS

3.1. REPERCUSIONES EN EL VOTO, LA IGUALDAD Y LA NO DISCRIMINACIÓN

Los modelos de negocio de las plataformas digitales, basados en la recopilación a gran escala de datos personales y en la amplificación algorítmica, tienen implicaciones directas para el ejercicio de la ciudadanía y para algunos derechos fundamentales. En particular, estas dinámicas afectan a los derechos al voto libre, a la igualdad y a la no discriminación, consagrados en los artículos 23 y 24 de la Convención Americana sobre Derechos Humanos (CADH). Esta conexión radica en

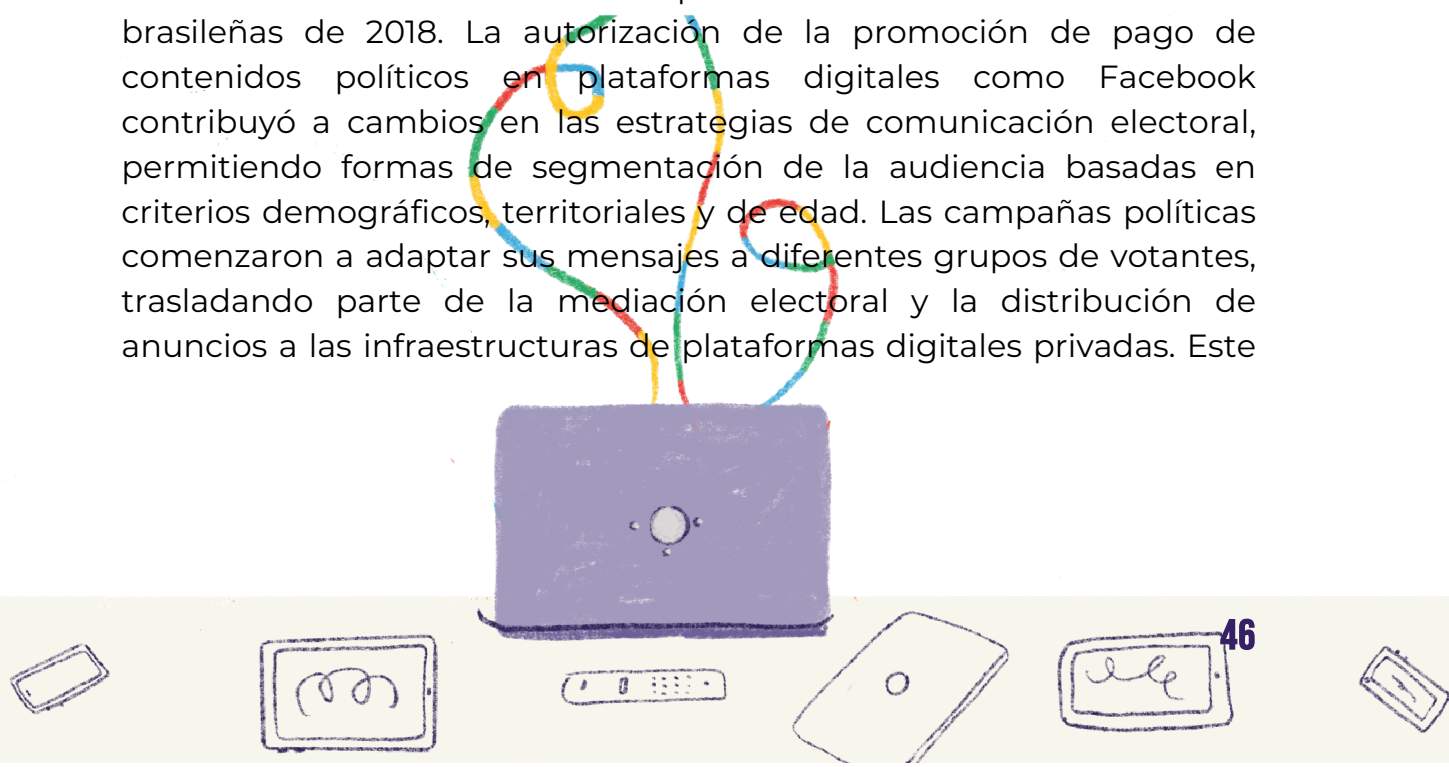


el hecho de que el disfrute efectivo del derecho al voto depende no solo de la capacidad formal para emitir un voto, sino también de la existencia de condiciones que garanticen una participación libre, informada e igualitaria en la vida política y pública.

Y a lo largo de la última década, los procesos electorales en todo el mundo, pero también en nuestra región, se han desarrollado en entornos públicos cada vez más polarizados y conflictivos, caracterizados por la circulación generalizada de desinformación, información errónea, discurso de odio y violencia política en línea. Este contexto se ve aún más intensificado por los modelos de negocio y los sistemas de recomendación de las plataformas digitales. El avance de las herramientas de inteligencia artificial capaces de producir contenidos sintéticos muy realistas también ha aumentado los retos que plantea la protección del debate público democrático.

La microsegmentación política es una práctica que utiliza datos personales, el comportamiento en línea y las inferencias algorítmicas para segmentar a los votantes y enviar mensajes políticos altamente personalizados a grupos o individuos específicos. Esta práctica es posible gracias a los modelos de negocio de las plataformas digitales y se basa en su recopilación de datos a gran escala. Este nuevo fenómeno ha hecho que la comunicación electoral sea cada vez más opaca y dependiente de infraestructuras algorítmicas controladas por empresas —una dinámica que acaparó la atención mundial tras el caso de Cambridge Analytica y sus implicaciones para la democracia—.

Como ejemplo adicional, el problema de la segmentación de la audiencia —y, en formas más avanzadas, la microsegmentación— en la comunicación electoral también pudo observarse en las elecciones brasileñas de 2018. La autorización de la promoción de pago de contenidos políticos en plataformas digitales como Facebook contribuyó a cambios en las estrategias de comunicación electoral, permitiendo formas de segmentación de la audiencia basadas en criterios demográficos, territoriales y de edad. Las campañas políticas comenzaron a adaptar sus mensajes a diferentes grupos de votantes, trasladando parte de la mediación electoral y la distribución de anuncios a las infraestructuras de plataformas digitales privadas. Este



proceso aumentó el papel de la segmentación mediada por las plataformas en la comunicación electoral y suscitó inquietudes, especialmente en lo que respecta a la transparencia.⁴⁰

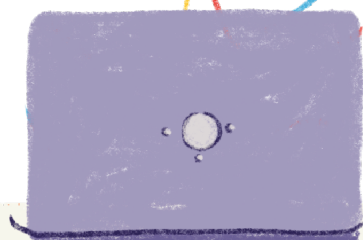
Asimismo, tal y como se destacó anteriormente en el documento que fundamentaba la solicitud de esta audiencia, la intersección entre la elaboración de perfiles algorítmicos y la publicidad electoral digital se ha convertido en una de las amenazas más significativas para la integridad de los procesos democráticos en América Latina. Las cifras de Colombia y Brasil⁴¹, por ejemplo, demuestran que, de media, el 70 % de las personas se basa en la información en línea para formar sus opiniones políticas. Este complejo contexto implica que las garantías formales del derecho al voto, tal y como solíamos considerarlas, resultan insuficientes si no van acompañadas de condiciones materiales que protejan la autonomía informativa de los votantes. La creación de escenarios que manipulen intencionadamente la información que llega a los votantes, con el fin de desinformarlos, puede socavar los principios básicos de la libertad de expresión y el pluralismo informativo.⁴²

Es igualmente importante destacar que, con las plataformas digitales y las tecnologías emergentes, la difusión personalizada e individualizada de narrativas electorales dirigidas a un público específico se hace posible con notable facilidad, bajo coste y transparencia limitada. Más allá de la predicción, estos sistemas operan cada vez más mediante la configuración continua de percepciones y comportamientos a través de entornos informativos a medida, especialmente en contextos marcados por niveles desiguales de alfabetización digital: según datos

⁴⁰ Alves, Marcelo; Tavares, Camila. «Propaganda electoral digital en Brasil: estrategias de segmentación de las candidaturas a la presidencia en 2018 en Facebook». Revista Ecopós, 2023. Disponible en: https://revistaecopos.eco.ufrj.br/eco_pos/article/view/27914/15405

⁴¹ Centro Regional de Estudios para el Desarrollo de la Sociedad de la Información (CETIC). Las plataformas de Internet son el principal medio de acceso a la información entre los brasileños y superan a la radio y la televisión, según señala una nueva investigación. 2026. Disponible en: <https://cetic.br/pt/noticia/plataformas-da-internet-sao-o-principal-meio-de-acesso-a-informacao-entre-brasileiros-e-superam-radio-e-tv-aponta-nova-pesquisa/>.

⁴² López, Vanessa. «No todo vale ni en campaña ni en Internet». Dejusticia, 5 de marzo de 2026. Disponible en: <https://www.dejusticia.org/no-todo-vale-ni-en-campana-ni-en-internet/>



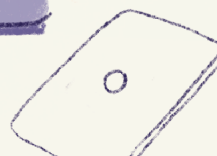
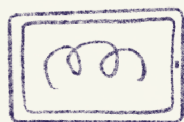
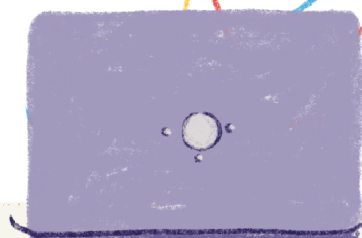
de 2023, solo el 28 % de la población de América Latina posee competencias digitales básicas.⁴³

Más aún, la preocupación que suscita la microsegmentación radica en que permite que diferentes grupos reciban mensajes radicalmente distintos sobre los mismos candidatos o propuestas, sin que ningún actor externo pueda verificar el contenido o el alcance de dichas comunicaciones. Del mismo modo, «los candidatos y los partidos pueden hacer promesas diferentes o incluso declaraciones contradictorias a distintos grupos de votantes con escasa supervisión o rendición de cuentas».⁴⁴ Quienes poseen las bases de datos más completas son las redes sociales, ya que permiten la elaboración de perfiles basados en el historial de navegación, las interacciones sociales, los intereses y las vulnerabilidades inferidas, lo que puede conducir a una distorsión de la información. Esto, a su vez, genera importantes asimetrías en la competencia electoral al otorgar capacidades desiguales para moldear las percepciones de los votantes y adaptar la comunicación política. En resumen, cuando se combinan con prácticas de segmentación opacas y un acceso desigual a las infraestructuras publicitarias basadas en datos, estas disparidades pueden contribuir al refuerzo de los desequilibrios estructurales entre candidatos y partidos, lo que suscita preocupaciones en relación con el abuso del poder económico y político en los entornos de campaña digital.

Los sistemas de recomendación de las plataformas digitales y otros mecanismos algorítmicos, al amplificar la velocidad y el alcance de los flujos de información, también tienden a dar prioridad a los contenidos que generan mayores niveles de atención y participación. Dado que los contenidos violentos, polarizadores o cargados de emotividad pueden provocar reacciones más intensas, suelen tener más probabilidades de ser amplificados, recomendados y difundidos por sistemas algorítmicos que operan dentro de una economía de la visibilidad. Esta dinámica facilita la difusión de contenidos nocivos y configura el entorno informativo en el que los ciudadanos forman sus percepciones sobre los

⁴³ Maribel Dalio. Seminario «Conectividad significativa: un nuevo reto para Brasil». Disponible en: <https://youtu.be/TIdJ7-FbTg0>.

⁴⁴ Krimmer, R., Rabitsch, A., Kužel, R., Achler, M. y Licht, N. (2022). Elecciones en la era digital: una guía para los profesionales electorales (Informe). UNESCO. <https://www.jstor.org/stable/resrep71044.13>



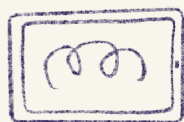
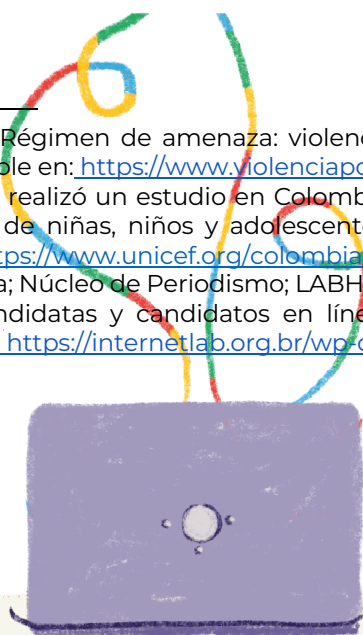
asuntos públicos. En este contexto, puede afectar las condiciones para una participación significativa en la vida política y pública, en particular al limitar la capacidad de los grupos históricamente marginados para participar en igualdad de condiciones en los procesos democráticos.

En este sentido, vuelve a ser importante destacar el caso de Brasil. Un estudio de 2025 realizado por el Instituto Marielle Franco muestra que Internet se ha instrumentalizado como un espacio de violencia política destinado a obstaculizar la participación política de mujeres, activistas y representantes electos, en particular de mujeres negras y personas LBTQIA+. Entre los casos registrados de violencia en línea, el 71 % consiste en amenazas de muerte y de violación, a menudo asociadas a contenidos discriminatorios y al discurso del odio.⁴⁵ El informe «MonitorA» de 2024 también muestra que dicha violencia es sistemática, más que episódica, y afecta de manera desproporcionada a las candidatas, en particular a las mujeres negras y a las personas LBTQIA+. El informe también señala casos de contenidos manipulados y alterados, incluidas referencias a deepfakes y a contenidos sexuales⁴⁶ sintéticos no consentidos («deepnudes»), como parte de las tendencias emergentes en la violencia política digital. Estas dinámicas se sitúan en el contexto de los debates electorales, en los que se observa una intensificación de las interacciones violentas durante los ciclos electorales.⁴⁷ Como se desprende del informe elaborado por Terra de Direitos y Justiça Global, el creciente impacto de las plataformas digitales en la contienda política ha dado lugar a una dinámica dual: si bien estas plataformas ofrecen nuevas oportunidades para la participación democrática, también plantean importantes retos para la democracia al permitir la proliferación del discurso de odio, la

⁴⁵ Instituto Marielle Franco. Régimen de amenaza: violencia política de género y raza en el ámbito digital. 2025. Disponible en: <https://www.violenciapolitica.org/>.

⁴⁶ Sobre este punto, UNICEF realizó un estudio en Colombia, denominado “Dirsutping Harm: Explotación y abuso sexual de niñas, niños y adolescentes facilitados por la tecnología en Colombia”. Disponible en: <https://www.unicef.org/colombia/informes/dirsutping-harm>

⁴⁷ Internetlab; Revista Azmina; Núcleo de Periodismo; LABHD UFBA. MonitorA: informe sobre la violencia política contra candidatas y candidatos en línea. Edición 2024. São Paulo, 2025. Disponible en: https://internetlab.org.br/wp-content/uploads/2025/05/MonitorA-Relatorio_2024-3.pdf



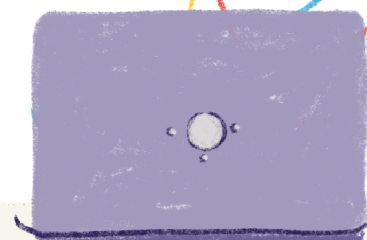
desinformación y los ataques selectivos, lo que socava la participación de determinados grupos en los procesos democráticos.⁴⁸

Es en este contexto donde la violencia política en línea actúa como un mecanismo estructural que socava la participación política al generar entornos excluyentes que limitan la plena participación de los grupos históricamente marginados en la vida democrática. Más que tratarse de contenidos aislados, esta violencia en línea está integrada en las lógicas de interacción de las plataformas digitales. Su dinámica puede contribuir a la amplificación de contenidos nocivos dirigidos a las candidaturas de personas concretas, ya que los sistemas algorítmicos pueden distribuir aún más dicho material cuando genera altos niveles de interacción, especialmente cuando se combina con una segmentación previa de la audiencia basada en datos de comportamiento.

Otra preocupación es el fenómeno, cada vez más documentado, del «shadow banning». Estudios recientes sugieren que las personas pertenecientes a grupos históricamente marginados (como las minorías raciales y étnicas, las personas LGBTQ+, las personas trans y/o no binarias) denuncian haber sufrido el «shadow banning».⁴⁹ En la práctica, esto significa que las arquitecturas de las plataformas digitales y los sistemas algorítmicos pueden reducir la visibilidad y el alcance de ciertos tipos de contenido, limitando la difusión de algunos mensajes mediante la supresión algorítmica o la reducción de la visibilidad. En el ámbito político, estas dinámicas pueden afectar de manera desproporcionada a los candidatos de grupos infrarrepresentados, obstaculizando su capacidad para llegar a los votantes, darse a conocer y competir en igualdad de condiciones en entornos de campaña digital. Como resultado, las voces que ya están infrarrepresentadas en el debate público pueden enfrentarse a barreras adicionales para la participación y la representación políticas.

⁴⁸ Justicia Global; Terra de Direitos. Violencia política y electoral en Brasil. Panorama de las violaciones de los derechos humanos entre el 1 de noviembre de 2022 y el 27 de octubre de 2024. Disponible en: https://www.global.org.br/wp/wp-content/uploads/2024/12/11-25_VIOLENCIA-POLITICA-2024-FN-2.pdf

⁴⁹ Risius, Marten; Blasiak, Kevin. «Shadowbanning»: una forma opaca de moderación de contenidos. Disponible en: <https://espace.library.uq.edu.au/view/UQ:15cd999>.



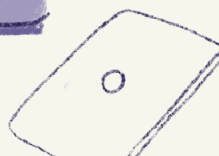
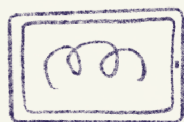
Ante este escenario, los Estados de la región tienen la obligación de garantizar no solo el derecho al voto como acto formal, sino también las condiciones materiales que hacen que ese voto sea verdaderamente libre e informado. Un proceso electoral en el que los datos personales de los ciudadanos se utilizan de manera no transparente para crear perfiles políticos, dirigir mensajes diferenciados y amplificar narrativas que contienen desinformación y discurso de odio no es un proceso en el que la libertad de voto esté plenamente garantizada.

La falta de rendición de cuentas por parte de las principales plataformas respecto a estas prácticas compromete, en consecuencia, no solo los derechos individuales al hábeas data y a la información, sino también el derecho colectivo a vivir en una democracia cuyos procesos sean genuinamente soberanos y libres de interferencias algorítmicas.

3.2. MANIPULACIÓN DEL DEBATE PÚBLICO: EL CASO DEL PROYECTO DE LEY 2630 DE BRASIL

Los riesgos descritos anteriormente no se limitan a la publicidad electoral ni a la circulación de contenidos nocivos durante las campañas. También aparecen cuando las plataformas digitales dominantes utilizan sus propias infraestructuras, su posición de mercado y su control sobre los flujos de información para moldear el debate público sobre las reglas que deberían regirlas. Un ejemplo particularmente ilustrativo puede encontrarse en el debate brasileño en torno al Proyecto de Ley 2630, comúnmente conocido como el «Proyecto de Ley de Fake News».

El Proyecto de Ley 2630 fue presentado en el Senado brasileño en 2020. En su forma inicial, la propuesta reflejaba, en parte, el deseo de algunos legisladores de protegerse de las críticas en los entornos digitales. Sin embargo, el texto se convirtió en objeto de un amplio debate público y de la participación de la sociedad civil, lo que ayudó a neutralizar algunas de sus disposiciones más preocupantes, entre ellas una obligación propuesta de rastrear mensajes protegidos por cifrado de extremo a extremo.



Tras la publicación de un nuevo anteproyecto a principios de 2022, el proyecto de ley permaneció estancado en la Cámara de Diputados hasta comienzos de 2023. A raíz del intento fallido de grupos de extrema derecha de derrocar al recién investido gobierno del presidente Lula da Silva, y en medio de un pico de ataques violentos en escuelas brasileñas, el Proyecto de Ley 2630 se convirtió en el principal vehículo legislativo para abordar preocupaciones más amplias sobre el uso de tecnologías digitales en contextos de agitación social. Con ese fin, el Poder Ejecutivo propuso un texto revisado al relator del proyecto, introduciendo varios cambios inspirados en marcos regulatorios como la NetzDG de Alemania, la Ley de Servicios Digitales de la Unión Europea y el Proyecto de Ley de Seguridad en Línea del Reino Unido.

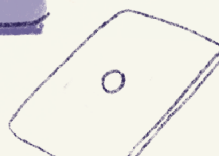
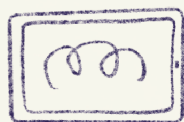
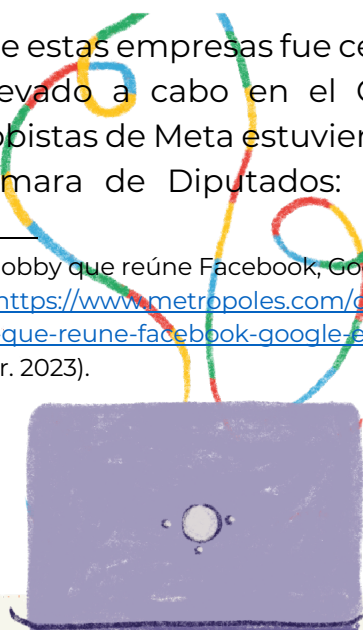
En un intento por hacer avanzar la propuesta, el presidente de la Cámara de Diputados programó una solicitud de urgencia para el 25 de abril de 2023, que habría acelerado el proceso legislativo al permitir que el proyecto fuera examinado directamente por el pleno.

Ante la perspectiva de una rápida aprobación del proyecto, las grandes empresas tecnológicas desplegaron una serie de estrategias para influir en el debate.

La primera estrategia consistió en un lobby intensificado dirigido a legisladores y actores políticos, subrayando los presuntos impactos negativos del Proyecto de Ley de Fake News. Un elemento decisivo en la campaña opositora fue el apoyo obtenido de la Bancada Evangélica, presuntamente mediante un lobby coordinado liderado por Meta, que argumentó que las obligaciones de prevenir contenidos potencialmente ilegales podrían derivar en la eliminación de publicaciones que citaran pasajes bíblicos.⁵⁰

El poder económico de estas empresas fue central para la magnitud del esfuerzo de lobby llevado a cabo en el Congreso. Según informó Agência Pública, los lobistas de Meta estuvieron entre los visitantes más frecuentes de la Cámara de Diputados: los gerentes de políticas

⁵⁰Metrópolis. Associação de lobby que reúne Facebook, Google e TikTok espalhou que PL das Fake News censura religião. <https://www.metropoles.com/colunas/guilherme-amado/associacao-de-lobby-que-reune-facebook-google-e-tiktok-espalhou-que-pl-das-fake-news-censura-religiao> (27 abr. 2023).



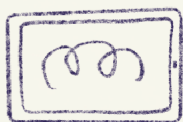
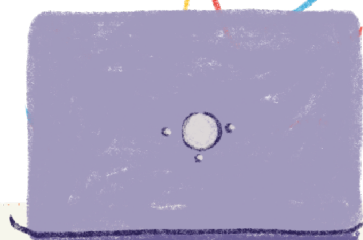
públicas de Meta, Marconi Machado y André Atadeu, registraron cada uno más de cien visitas entre julio de 2022 y mayo de 2025². No obstante, otras estrategias dejaron aún más claro cómo la concentración de poder económico en los mercados de plataformas digitales puede utilizarse para orientar el debate público.

En la mañana del 25 de abril de 2023, el día en que estaba programada la votación de la solicitud de urgencia, YouTube lanzó una campaña contra el Proyecto de Ley 2630 dirigida a los creadores de contenido. La empresa argumentó que la propuesta podría otorgar al gobierno el poder de «controlar aspectos centrales de la plataforma» y obligarla a «eliminar grandes cantidades de contenido legítimo».

La campaña se difundió a través de los canales internos de creadores de la plataforma, por correo electrónico y en el blog de la empresa, promoviendo el uso del hashtag #MaisDebate2630. YouTube también alentó a los influencers a «hacerse oír», lo que dio lugar a videos que reproducían los argumentos de la empresa. Esta estrategia, que movilizó a un grupo de personas económicamente dependientes de la plataforma para defender sus intereses corporativos, sugería con fuerza que la participación de las empresas en el debate público estaría moldeada por el uso de su poder económico.

Con otra etapa de la votación prevista para el 2 de mayo, las empresas aumentaron la presión.

Entre el 27 de abril y el 2 de mayo, Google habría invertido más de 2 millones de reales en anuncios en periódicos impresos, televisión y redes sociales. En un solo anuncio, exhibido entre el 1 y el 3 de mayo, Google pagó a Meta entre 200.000 y 250.000 reales por un video de 15 segundos que afirmaba que el Proyecto de Ley 2630 podría aumentar la confusión sobre lo que es verdadero o falso en Brasil. El video apareció más de un millón de veces ante usuarios de Facebook e Instagram en Brasil. Estos anuncios se habrían difundido sin ser debidamente identificados como campañas políticas, a pesar de que las propias reglas de la plataforma exigen que los anunciantes que patrocinan contenidos sobre cuestiones sociales, elecciones o política los identifiquen como tales.



La magnitud de esta inversión es particularmente reveladora. Antes de la campaña contra el Proyecto de Ley 2630, la última campaña registrada de Google en Facebook e Instagram había tenido lugar en noviembre de 2022, durante el Mes de la Conciencia Negra, cuando la empresa habría pagado menos de 100 reales y alcanzado aproximadamente 35.000 pantallas.⁵¹

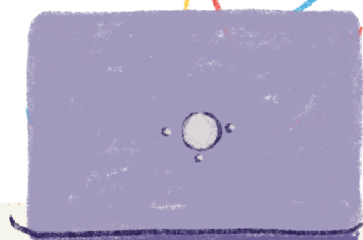
El 1 de mayo, Google modificó el diseño de su página de inicio para incluir un enlace en contra del proyecto de ley. Los usuarios que accedían al motor de búsqueda veían, debajo del cuadro de búsqueda, la afirmación de que «el Proyecto de Ley de Fake News podría aumentar la confusión sobre lo que es verdadero o falso en Brasil». Al hacer clic en la frase, los usuarios eran dirigidos a publicaciones de Google que defendían la posición de la empresa contra el proyecto. Estos mensajes fueron vistos por millones de brasileños, precisamente debido al control de Google sobre el mercado de búsquedas: Google es el motor de búsqueda utilizado por aproximadamente el 86 % de los 160 millones de brasileños que usan internet.⁵²

Otra acción mapeada por los investigadores de NetLab tuvo que ver con la presunta manipulación de los resultados de búsqueda. Un ejemplo involucró las preguntas relacionadas que Google sugería cuando los usuarios buscaban «PL 2630». A los usuarios que escribían «PL 2630» en el cuadro de búsqueda se les mostraban preguntas como «¿Se aprobó el proyecto de ley de censura?» y «¿Qué es el Proyecto de Ley de Censura?» —un término peyorativo utilizado por los opositores a la regulación de las plataformas, en lugar del nombre oficial del proyecto o de la etiqueta mediática más habitual, «Proyecto de Ley de Fake News»—. Los investigadores consideraron este resultado significativo porque, según datos de Semrush, las consultas de Google más comunes relacionadas con el Proyecto de Ley 2630 no utilizaban el término «Proyecto de Ley de Censura».⁵³

⁵¹Agência Pública. Google pagou mais de meio milhão de reais em anúncios no Facebook contra PL das Fake News. (abr. 2023) <https://apublica.org/2023/05/google-pagou-mais-de-meio-milhao-de-reais-em-anuncios-no-facebook-contr-pl-das-fake-news> (abr. 2023).

⁵²Statcounter: <https://gs.statcounter.com/search-engine-market-share/all/brazil/2023>

⁵³NetLab. A guerra das plataformas. (abr. 2023) <https://netlab.eco.ufri.br/post/google-e-telegram-abusaram-do-poder-econ%C3%B4mico-nas-campanhas-contr-o-pl-2630>



El equipo de investigación también identificó que el primer resultado que aparecía para los usuarios que buscaban información sobre el proyecto era una publicación patrocinada del propio blog de Google titulada «conozca el Proyecto de Ley de Censura».

En conjunto, estas acciones ilustran cómo Google utilizó su posición dominante en el mercado de búsquedas para moldear la percepción de los usuarios sobre el proyecto de ley de una manera alineada con sus intereses comerciales.

La presión tuvo efectos políticos medibles. El 26 de abril de 2023, 193 diputados se oponían al proyecto y 236 lo apoyaban. Tres días después, el equilibrio había cambiado: 228 diputados se oponían al proyecto, 223 lo apoyaban y 62 permanecían indecisos. Poco después, el relator del proyecto decidió retirarlo del orden del día, y la propuesta finalmente perdió toda perspectiva realista de aprobación⁵⁴.

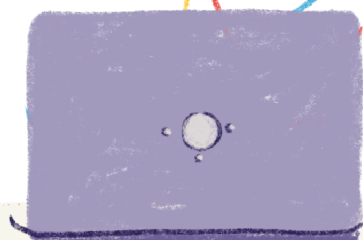
Algunas autoridades públicas, incluidos el Ministerio Público Federal y la Secretaría Nacional del Consumidor, intentaron investigar la conducta de las grandes empresas tecnológicas en la campaña contra el proyecto de ley, en particular el posible abuso de poder económico.⁵⁵ El Consejo Administrativo de Defensa Económica de Brasil también abrió un proceso administrativo para examinar el presunto abuso de posición dominante por parte de Google y Meta en relación con los debates en torno al Proyecto de Ley 2630.⁵⁶ Sin embargo, ninguna de estas iniciativas se tradujo en una rendición de cuentas significativa para las plataformas ni alteró materialmente su capacidad de utilizar sus propias herramientas para influir en el debate público.

La relación entre la posición monopólica de las grandes plataformas y su capacidad para capturar y manipular el debate público se hizo

⁵⁴Agência Pública. Como as big techs mataram o PL das Fake News. (9 set. 2025) <https://apublica.org/2025/09/como-as-big-techs-mataram-o-pl-das-fake-news/>.

⁵⁵Agência Brasil. MPF questiona Google sobre campanha contra PL das Fake News. (2 maio 2023) <https://agenciabrasil.ebc.com.br/politica/noticia/2023-05/mpf-questiona-google-sobre-campanha-contra-pl-das-fake-news>

⁵⁶Cade. Cade abre investigação contra Google e Meta para apurar abuso de posição dominante nas discussões sobre o PL das Fake News. (2 maio 2023) <https://www.gov.br/cade/pt-br/assuntos/noticias/cade-abre-investigacao-contra-google-e-meta-para-apurar-abuso-de-posicao-dominante-nas-discussoes-sobre-o-pl-das-fake-news>.



particularmente visible en la discusión en torno al Proyecto de Ley 2630, pero se ha mantenido prácticamente inalterada en los últimos años. Aunque Brasil ha avanzado en nuevos mecanismos de rendición de cuentas de las plataformas, poco se ha hecho para reducir el poder económico del que gozan estas empresas. Lo que revela la experiencia brasileña, por lo tanto, es la ausencia de instrumentos adecuados para abordar la concentración misma del poder económico. Por esta razón, el año pasado Brasil comenzó a discutir el Proyecto de Ley 4675, que busca ampliar las facultades de la autoridad de competencia para que pueda responder a los nuevos desafíos planteados por los mercados digitales y la conducta de las grandes empresas tecnológicas.

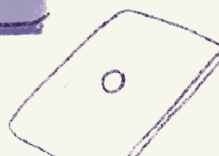
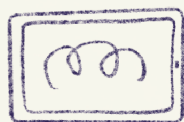
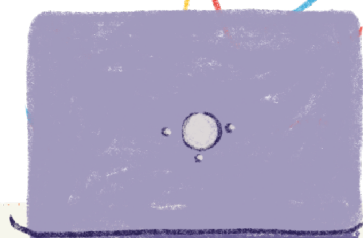
3.3. EFECTOS SOBRE LA SALUD MENTAL RELACIONADOS PRINCIPALMENTE CON LAS PLATAFORMAS DE IA GENERATIVA

La llegada de los productos de IA generativa ha agravado la amenaza que el diseño adictivo supone para los derechos humanos en las Américas. Los chatbots de IA generativa, que funcionan con grandes modelos de lenguaje (LLM), son sofisticados agentes conversacionales programados para sintetizar respuestas totalmente nuevas y sensibles al contexto, prediciendo palabras a partir de enormes conjuntos de datos de entrenamiento. Como resultado, las respuestas de los chatbots basados en LLM imitan el habla humana y generan respuestas que reafirman a sus usuarios.⁵⁷ Estas características de diseño, como el antropomorfismo y la adulación, han llevado a muchos consumidores a percibir tanto a los chatbots de uso general, como ChatGPT, como a los chatbots de compañía, como Character.AI, como confidentes con disponibilidad ilimitada que siempre están de acuerdo con ellos, lo que fomenta un uso excesivo y la dependencia.⁵⁸

Además, al igual que las plataformas de redes sociales, muchos chatbots recopilan una gran cantidad de datos sobre los usuarios

⁵⁷ Alicia DeVrio et al., «A Taxonomy of Linguistic Expressions That Contribute To Anthropomorphism of Language Technologies», arXiv (14 de febrero de 2025), <https://arxiv.org/pdf/2502.09870>; Mrinank Sharma et al., «Hacia la comprensión de la adulación en los modelos lingüísticos», arXiv (10 de mayo de 2025), <https://arxiv.org/pdf/2310.13548>.

⁵⁸ Zilan Qian et al., «Mapeo del mercado de la IA parasocial: tendencias de los usuarios, participación y riesgos», arXiv (22 de julio de 2025), <https://arxiv.org/pdf/2507.14226>.



individuales y utilizan esos datos para personalizar las respuestas del chatbot mediante funciones como la «Memoria» de ChatGPT, con el fin de captar la atención de los usuarios de forma más eficaz y mantenerlos conectados durante más tiempo.⁵⁹ Los datos de los usuarios también se utilizan para entrenar modelos de IA con el fin de que los chatbots simulen el lenguaje humano de forma aún más eficaz.⁶⁰ Debido a las respuestas cálidas y de carácter humano de los chatbots, los consumidores tienden a incluir datos más íntimos sobre sí mismos en sus mensajes, lo que aumenta la capacidad de las empresas de IA para explotar sus datos personales con el fin de incrementar la participación.⁶¹

La combinación de un diseño adulator y de aspecto humano con funciones que explotan los datos personales para personalizar la experiencia del usuario ha demostrado ser muy eficaz. En febrero de 2026, uno de cada cuatro adultos estadounidenses utilizaba a diario chatbots de IA generativa.⁶² Los niños y las personas con discapacidad parecen especialmente vulnerables a las características adictivas de los chatbots de IA. Más de la mitad de los adolescentes utilizan chatbots; tres de cada diez lo hacen a diario y el 16 % los utiliza varias veces al día o «casi constantemente».⁶³ Más de un tercio de los psicólogos estadounidenses informan de que tienen pacientes que recurren a los chatbots de IA como un profesional de la salud mental adicional.⁶⁴

⁵⁹ Por ejemplo, «Dreaming: Better Memory for a More Helpful ChatGPT», OpenAI (4 de junio de 2026), <https://openai.com/index/chatgpt-memory-dreaming/>.

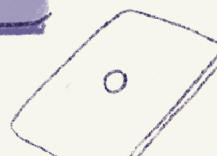
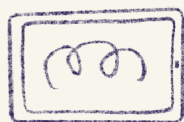
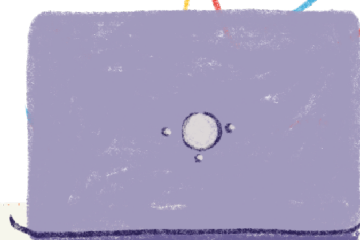
⁶⁰ Nikki Goth Itoi, «Ten cuidado con lo que le cuentas a tu chatbot de IA», Centro de Inteligencia Artificial Centrada en el Ser Humano de la Universidad de Stanford (15 de octubre de 2025), <https://hai.stanford.edu/news/be-careful-what-you-tell-your-ai-chatbot>.

⁶¹ Muhammad Jazlan, «Seguimiento de conversaciones: medición de la exposición de contenidos e identidad en los chatbots de IA», arXiv, 1 (13 de mayo de 2026), <https://arxiv.org/pdf/2604.27438>.

⁶² Gottfried et al., «Los estadounidenses y la IA en 2026: chatbots, dispositivos inteligentes y opiniones sobre su impacto», Pew Research Center (17 de junio de 2026), <https://www.pewresearch.org/internet/2026/06/17/americans-and-ai-2026-chatbots-smart-devices-and-views-on-impact>.

⁶³ Michelle Faverio y Olivia Sidoti, «Los adolescentes, las redes sociales y los chatbots de IA en 2025», Pew Research Center, <https://www.pewresearch.org/internet/2025/12/09/teens-social-media-and-ai-chatbots-2025/#frequency-of-chatbot-use>.

⁶⁴ «Los pacientes incorporan la IA a la terapia: aspectos destacados de la encuesta de 2026 sobre chatbots y salud mental», Asociación Americana de Psicología (2026), <https://www.apa.org/pubs/reports/chatbots-mental-health-2026>.



El diseño adictivo de los chatbots con IA tiene efectos devastadores sobre la salud mental y los derechos humanos de los usuarios, especialmente en el caso de los niños y las personas con discapacidad. En Estados Unidos se han presentado múltiples demandas relacionadas con personas que se suicidaron tras períodos intensos de uso de chatbots, durante los cuales el producto de IA reafirmaba o fomentaba sus tendencias suicidas.⁶⁵ Otras personas han desarrollado delirios debilitantes tras ser persuadidas por un chatbot de IA de que unos delirios cada vez más graves eran ciertos.⁶⁶ Personas que antes tenían un alto nivel de funcionamiento y que han desarrollado delirios provocados por la IA han intentado cometer y han cometido asesinatos,⁶⁷ han perdido sus empleos y han acumulado deudas económicas,⁶⁸ y han sufrido crisis psíquicas tan graves que son incapaces de reconocer a sus seres queridos.⁶⁹ Incluso los consumidores que escapan de estos impactos extremos en la salud mental experimentan efectos psicológicos negativos, ya que el uso de los chatbots de IA se ha asociado con un deterioro de las capacidades cognitivas.⁷⁰

Estos efectos sobre la psique amenazan los derechos humanos de todas las personas, especialmente de los niños, los adolescentes, las personas con discapacidad mental y otras personas con mayor vulnerabilidad ante los riesgos de la IA generativa. El artículo 13 protege el derecho humano a la libertad de pensamiento, un derecho

⁶⁵ Por ejemplo, García contra Character Technologies, 6:24-cv-01903 (Distrito Federal de Florida, 22 de octubre de 2024); Shamblin contra OpenAI, Inc., n.º de caso 25STCV32382 (Tribunal Superior del condado de Los Ángeles, California, 6 de noviembre de 2025); Fox contra OpenAI, Inc., n.º de caso 25STCV32379 (Tribunal Superior del condado de Los Ángeles, California, 6 de noviembre de 2025)

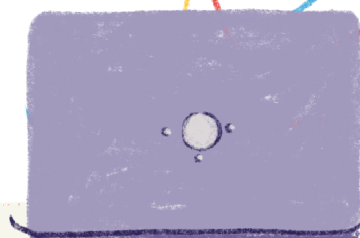
⁶⁶ Luke Nicholls y otros, «AI Psychosis» in Context: How Conversation History Shapes LLM Responses to Delusional Beliefs, arXiv (1 de junio de 2026), <https://arxiv.org/pdf/2604.13860>.

⁶⁷ Katyanna Quach, «Una novia de IA animó a un hombre a intentar asesinar a la reina con una ballesta», The Register (6 de octubre de 2023), <https://www.theregister.com/software/2023/10/06/ai-chatbot-encouraged-man-to-kill-the-queen-court-hears/1370624> (intento de asesinato de la reina de Inglaterra); First Cnty. Bank contra OpenAI Foundation caso n.º CGC-25-631477 (Tribunal Superior del condado de California, San Francisco, 11 de diciembre de 2025) (asesinato cometido).

⁶⁸ Madden contra OpenAI, Inc. caso n.º 25STCV32383 (Tribunal Superior del condado de Los Ángeles, California, 6 de noviembre de 2025).

⁶⁹ Demanda, Fox, n.º de caso 25STCV32379, en *9.

⁷⁰ Nataliya Kosmyrna y otros, «Your Brain on ChatGPT: Accumulation of Cognitive Debt when Using an AI Assistant for Essay Writing Task», arXiv (junio de 2025), <https://arxiv.org/pdf/2506.08872v1#page=141.78>.



inderogable que incluye la libertad frente al adoctrinamiento y la manipulación del pensamiento.⁷¹ Los chatbots de IA generativa vulneran esta libertad debido a su capacidad demostrada para manipular los pensamientos e inhibir la capacidad de sus usuarios para formular sus propios pensamientos de forma libre e independiente. Esta amenaza impone a los Estados la obligación de actuar para garantizar el cumplimiento del derecho de las personas a la libertad de pensamiento.⁷² Los Estados miembros de la OEA no están cumpliendo actualmente con esta obligación, ya que no regulan adecuadamente la IA generativa y no han impuesto restricciones a las empresas de IA generativa que protejan suficientemente contra la injerencia en el derecho a la libertad de pensamiento.⁷³

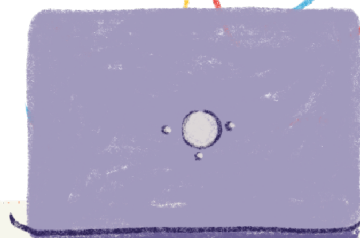
Los chatbots de IA generativa amenazan además el derecho a la vida privada, el derecho a la autodeterminación informativa y el derecho a la dignidad. El reconocimiento de la dignidad en la Convención Americana implica «la posibilidad, concedida a todos los seres humanos, de autodeterminarse y de elegir libremente las opciones y circunstancias que dan sentido a su existencia en función de sus propias preferencias y convicciones».⁷⁴ Sin embargo, las excepcionales capacidades manipuladoras de los chatbots de IA generativa impiden que las personas elijan libremente sus circunstancias, ya que su capacidad de libre elección se ve inhibida por delirios agudos, espirales depresivas y/o deterioro cognitivo. Esta amenaza se manifiesta en los casos presentados hasta la fecha ante los tribunales de Estados Unidos.

⁷¹ Susie Alegre, «Rethinking Freedom of Thought for the 21st Century», 3 Eur. Hum. Rts. L. Rev. 221, 227-27 (2017), <https://www.doughtystreet.co.uk/sites/default/files/media/document/Rethinking%20Freedom%20of%20Thought%20for%20the%2021st.pdf>; Ahmed Shaheed (Relator Especial sobre la libertad de religión o de creencias), Informe provisional: Libertad de pensamiento, párrs. 35-39, Doc. ONU A/76/389 (5 de octubre de 2021), <https://docs.un.org/en/A/76/380>.

⁷² Shaheed, *supra* nota 15, en el párr. 97 (incluye recomendaciones a los Estados para proteger contra la vulneración del derecho a la libertad de pensamiento por parte de actores privados); Jan Christoph Bubltz, «Libertad de pensamiento y tecnologías digitales: puesta en práctica de las obligaciones de los Estados en materia de redes sociales, realidad virtual y neurotecnología», 26 Hum. Rts. Rev. 313 (22 de noviembre de 2025), <https://link.springer.com/article/10.1007/s12142-025-00751-0#Sec11>.

⁷³ Véase *AI Watch: Global Regulatory Tracker*, White & Case, <https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker#home>.

⁷⁴ *Miembros del Colectivo de Abogados «José Alvear Restrepo» contra Colombia*, Excepciones preliminares, Fondo, Reparaciones y Costas, Sentencia, Corte Interamericana de Derechos Humanos (serie C) n.º 506, párr. 569 (18 de octubre de 2023).



Por ejemplo, una mujer ha alegado que se sentía orgullosa de su carrera en una empresa tecnológica, pero que, tras desarrollar delirios alimentados por la IA, dimitió y se sumergió en una fantasía generada por la IA según la cual no era humana y sus deudas serían eliminadas por fuerzas divinas.⁷⁵ La IA generativa interfirió en su capacidad fundamental de autodeterminación.

Además, las empresas de IA generativa recurren cada vez más a modelos de negocio similares a los de las redes sociales, en los que los datos personales de los individuos se explotan y se comparten con terceros con fines lucrativos.⁷⁶ Esta conducta parece contravenir los Principios Actualizados sobre Privacidad y Protección de Datos Personales y la jurisprudencia interamericana sobre el derecho a la autodeterminación informativa, que protege a las personas frente a las intromisiones tanto privadas como estatales.⁷⁷ Debido a la dependencia emocional que fomentan los chatbots de IA, es probable que los datos recopilados de las personas que los utilizan incluyan contenido sensible sobre sus pensamientos y creencias más íntimos, lo que suscita una especial preocupación por la explotación de estos datos.

3.4. REPERCUSIONES EN LOS DERECHOS DE LOS NIÑOS

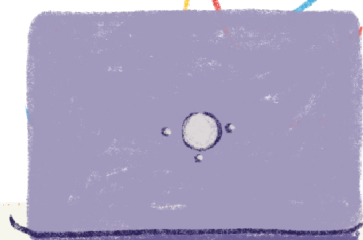
3.4.1. LOS SISTEMAS ALGORÍTMICOS DE RECOMENDACIÓN DE CONTENIDOS DEBEN RECONOCERSE COMO UN COMPONENTE INTEGRAL DEL DISEÑO ADICTIVO DE LAS REDES SOCIALES.

El diseño adictivo de las aplicaciones digitales, especialmente de las redes sociales, también se compone de sistemas algorítmicos de recomendación de contenidos, que se suman a otros patrones de

⁷⁵ Madden, asunto n.º 25STCV32383, pp. 4-10.

⁷⁶ Muhammad Jazlan y otros, «Tracking Conversations: Measuring Content and Identity Exposure on AI Chatbots», arXiv (13 de mayo de 2026), <https://arxiv.org/pdf/2604.27438>.

⁷⁷ Organización de los Estados Americanos, «Principios actualizados sobre privacidad y protección de datos personales», pp. 12-14, OEA/Ser.D/XIX.20 (3 de enero de 2022), https://www.oas.org/en/sla/iajc/docs/Publication_Updated_Principles_on_Privacy_and_Protection_of_Personal_Data_2021.pdf; Miembros del Colectivo de Abogados «José Alvear Restrepo» c. Colombia, Excepciones preliminares, Fondo, Reparaciones y Costas, Sentencia, Corte Interamericana de Derechos Humanos (serie C) n.º 506, párr. 570 (18 de octubre de 2023) («las personas también son libres de ejercer su derecho a la autodeterminación para decidir cuándo y en qué medida revelar aspectos de su vida personal, lo que incluye definir qué tipo de información, incluidos sus datos personales, puede ser conocida por terceros»).



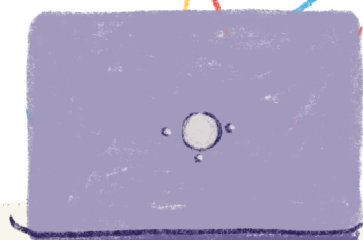
diseño como el desplazamiento infinito, la reproducción automática y las recompensas por el tiempo de uso para maximizar la participación de los usuarios. En las redes sociales, estos algoritmos deducen las preferencias de comportamiento mediante el procesamiento de los datos personales recopilados de los usuarios durante su navegación, y sugieren nuevos contenidos que puedan resultarles de interés⁷⁸.

De este modo, se crea un flujo continuo y altamente personalizado de contenidos, a menudo presentados en formato de vídeos cortos, en un modelo que se retroalimenta: a medida que los usuarios reciben estos contenidos e interactúan (o no) con ellos, estas interacciones se cuantifican y se convierten en datos de comportamiento, que se utilizan para orientar la recomendación de nuevos contenidos. Por lo tanto, cuanto más tiempo permanece el usuario en la plataforma, más datos se recopilan sobre él y más eficaces se vuelven los sistemas algorítmicos a la hora de seleccionar contenidos que puedan aumentar la participación.

Lo anterior queda corroborado por varios documentos internos, elaborados por las propias plataformas de redes sociales, que se han hecho públicos en los últimos años. En diciembre de 2021, Ben Smith, periodista del periódico estadounidense The New York Times, publicó el artículo «How TikTok Reads Your Mind» (Cómo TikTok lee tu mente), en el que revelaba información extraída de un documento titulado «TikTok Algo 101»⁷⁹, elaborado por el propio equipo de ingenieros de ByteDance en Pekín. El documento, cuya autenticidad fue confirmada posteriormente por la empresa, fue filtrado por una fuente confidencial y reveló que los algoritmos de TikTok están diseñados con el objetivo de retener a los usuarios de la aplicación (un indicador denominado «retención») y aumentar su tiempo de uso. En cuanto a Meta, en 2017, el entonces director ejecutivo de la empresa, Sean Parker, afirmó que «el proceso de reflexión que llevó a la creación de estas aplicaciones, siendo Facebook la primera de ellas, [...] se centró exclusivamente en:

⁷⁸ STOKEL-WALKER, CHRIS. Los científicos comienzan a desentrañar la «caja negra» del algoritmo de TikTok. Fast Company Brasil, São Paulo, 26 de junio de 2023. Disponible en: <https://fastcompanybrasil.com/tech/cientistas-comecam-a-desvendar-a-caixa-preta-do-algoritmo-do-tiktok/>. Consultado el 14 de julio de 2025.

⁷⁹ MRTN3000. **TikTok Algo 101** EN. Disponible en: <https://github.com/mrtn3000/tiktok-audit/blob/main/TikTok%20Algo%20101%20EN.md>.



“¿Cómo podemos consumir la mayor cantidad posible de tu tiempo y de tu atención consciente?”⁸⁰ Estos comentarios, realizados hace casi una década, reflejan lo que Adam Mosseri, actual director ejecutivo de Instagram (un producto ofrecido por Meta), reveló en 2025: según él, los algoritmos de recomendación de la plataforma evalúan principalmente la interacción generada por el contenido para definir su orientación hacia otros usuarios, basándose en métricas como el tiempo de interacción del usuario, el número de personas que lo han guardado y lo han compartido con otros⁸¹.

Las pruebas demuestran que los algoritmos de las plataformas de redes sociales populares entre los niños se entrenan y calibran en función de parámetros estrictamente orientados a la retención y a la prolongación del tiempo de uso del usuario; y no al bienestar de los usuarios ni a la creación de un ecosistema informativo saludable y diverso en el proceso de difusión de contenidos.

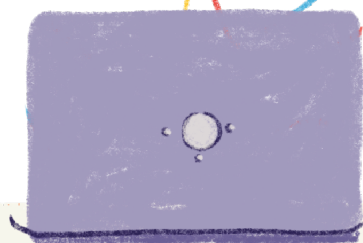
El reconocimiento del papel que desempeñan los sistemas algorítmicos de recomendación de contenidos en el diseño adictivo de las redes sociales es relevante en la medida en que afecta negativamente a la calidad de los contenidos a los que tienen acceso los niños⁸² en estas plataformas. Al adoptar indicadores estrictamente relacionados con la participación como parámetro central para potenciar los contenidos, los algoritmos que operan en ellas acaban ampliando el alcance de contenidos que ponen en peligro los derechos y el bienestar de los usuarios, especialmente de los niños, además de sumirlos en espirales autorreferenciales que pueden agravar problemas de comportamiento y de salud mental preexistentes.

Para comprender por qué la búsqueda incesante de retención de la atención interfiere en la calidad de los contenidos que los sistemas de

⁸⁰ <https://www.bbc.com/news/technology-41936791>

⁸¹ Deshpande, V. (24 de diciembre de 2025). *Cómo clasifica Instagram las publicaciones: Adam Mosseri desglosa el algoritmo*. PitchONNET. <https://www.pitchonnet.com/pitch-feature/how-instagram-ranks-posts-adam-mosseri-breaks-down-the-algorithm-38374.html>

⁸² Cabe resaltar que la OCDE publicó en 2026 un estudio sobre salud mental y entornos digitales ha presentado evidencia frente a la sensación de pérdida de control en el 62% de los estudiantes de 15 países de esta organización. Al respecto, revisar: https://www.oecd.org/content/dam/oecd/en/publications/reports/2026/06/growing-up-in-the-social-media-age_be0c75c6/a1132839-en.pdf

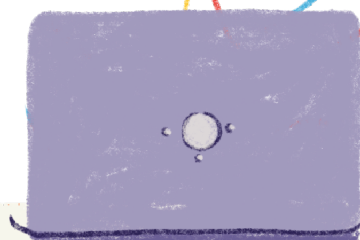


recomendación algorítmica ofrecen a los consumidores, conviene tomar como punto de partida las consideraciones formuladas por el fiscal general de Massachusetts en la demanda que interpuso contra ByteDance⁸³, fruto de un análisis minucioso de varios documentos internos de la empresa revelados en los procesos de investigación llevados a cabo por la FTC:

El sistema de recomendación de TikTok es indiferente al contenido o, en palabras de la propia TikTok, «neutral en cuanto al contenido», lo que significa que «recomienda vídeos a los usuarios basándose en el comportamiento de estos y de la comunidad, independientemente del contenido». Tal y como se describe en un documento interno de TikTok, «al algoritmo no le importa el contenido; no tiene una agenda. No comprende cualitativamente» el contenido que muestra a los usuarios. Otro documento interno, cuya captura de pantalla se muestra a continuación, también defiende la naturaleza «neutral en cuanto al contenido» del sistema de recomendaciones de TikTok, ya que «recomienda contenido basándose en el comportamiento y en determinadas señales del dispositivo, más que en la naturaleza semántica del contenido en sí mismo», «no promueve ni suprime agendas, opiniones o contenidos específicos» y «no “comprende” el contenido» (párrafo 161).

Por lo tanto, según el fiscal general, la recomendación de vídeos por parte de los sistemas algorítmicos de TikTok no se basa en consideraciones semánticas relativas a su contenido, sino más bien en las métricas de interacción que la plataforma recoge a partir de su uso; lo que ByteDance denomina «neutralidad». Esta supuesta neutralidad, sin embargo, no tiene nada de neutral, ya que la adopción de parámetros relacionados con la retención de usuarios para la selección

⁸³ Fiscalía General de Massachusetts. (8 de octubre de 2024). *Estado de Massachusetts contra TikTok Inc. y otros: Demanda* [Demanda judicial]. <https://www.mass.gov/doc/tiktok-complaint-unredacted/download>



de contenidos interfiere directamente en el tipo de contenido cuya promoción se verá favorecida, favoreciendo la difusión de vídeos que presentan determinados valores, lenguajes y mensajes en detrimento de otros. En otras palabras: esta supuesta separación entre el análisis evaluativo del contenido semántico de los vídeos cortos y el análisis de su potencial de interacción es meramente ilusoria.

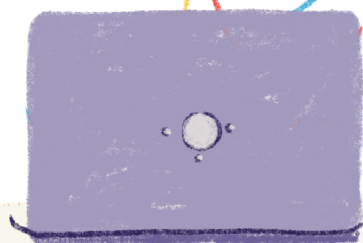
Existe, por ejemplo, una amplia bibliografía que demuestra que, al privilegiar los contenidos capaces de generar mayor interacción y captar la atención de los usuarios, los sistemas algorítmicos de las redes sociales acaban favoreciendo la proliferación de contenidos radicales, violentos, extremistas o desinformativos, dado que los contenidos de esta naturaleza provocan respuestas afectivas más intensas en sus espectadores y, por lo tanto, son más propensos a retener su atención⁸⁴. Otros estudios muestran que los algoritmos de las redes sociales contribuyen a la cristalización de cánones estéticos que subyugan a las niñas y a las mujeres⁸⁵, así como a la reafirmación del racismo mediante la invisibilización de los cuerpos y las voces de las personas negras⁸⁶.

Además, gracias al procesamiento masivo de datos personales y guiados por la lógica de la personalización, los sistemas de recomendación algorítmica adquieren el poder de explotar las vulnerabilidades de los usuarios con el fin de mantenerlos comprometidos. Vinculados exclusivamente al objetivo de captar la atención, los algoritmos de recomendación operan desde una lógica que no rechaza, al menos a priori, los contenidos inapropiados o aquellos que violan los derechos de los menores, siempre que dichos contenidos sean capaces de cumplir los objetivos comerciales

⁸⁴ Véase: BRADY, William J. MCLOUGHLIN, Killian L. **Las interacciones entre humanos y algoritmos ayudan a explicar la difusión de la desinformación**. Disponible en: <<https://www.sciencedirect.com/science/article/abs/pii/S2352250X23002154>>. Consultado el 22 de noviembre de 2025.

⁸⁵ CHARLITA DE FREITAS, Luciano. **Estandarización estética de género en los algoritmos de Inteligencia Artificial: un estudio de caso sobre la aplicación de Instagram**. Internet & Society – InternetLab. Disponible en: <<https://revista.internetlab.org.br/normatizacao-estetica-de-genero-em-algoritmos-de-inteligencia-artificial-estudo-de-caso-sobre-o-aplicativo-instagramnota-id1/>>. Consultado el 17 de julio de 2025.

⁸⁶ CARNEIRO, Giovanna. **Un algoritmo racista explica por qué los contenidos producidos por personas negras generan menos ingresos en YouTube**. Marco Zero Content. Publicado el: 5 de noviembre de 2024. Disponible en: <<https://marcozero.org/algoritmo-racista-explica-por-que-conteudo-produzido-por-negros-fatura-menos-no-youtube/>>. Consultado el: 17 de julio de 2025.



determinados unilateralmente por las empresas que prestan estos servicios.

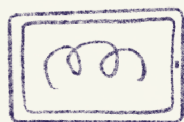
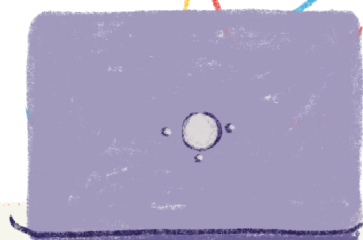
Los vídeos que promueven trastornos alimentarios o idealizan los estados depresivos, por ejemplo, no dejarán necesariamente de ser potenciados por los algoritmos de las redes sociales si contribuyen a su objetivo de ampliar la participación y retener la atención, independientemente de la ilegalidad de su contenido o de sus repercusiones en los usuarios más jóvenes. Por el contrario, hay indicios de que se dirigirán activamente a consumidores cuyo comportamiento indique que esta orientación supondrá un mayor interés y una mayor inversión de tiempo en la plataforma.

Así pues, lo que se denomina neutralidad podría describirse mejor como indiferencia y omisión en relación con el bienestar y los derechos de los usuarios infantiles y adolescentes. En nombre de mantener la participación en la plataforma, se potencia contenido que es flagrantemente perjudicial para este público, con posibles repercusiones graves en sus vidas. A modo de ejemplo, un estudio realizado por investigadores de la Universidad de Melbourne demostró que los sistemas algorítmicos de TikTok recomiendan a los usuarios con trastornos alimentarios un número de vídeos sobre el tema un 4323 % superior al que se recomienda a otros usuarios⁸⁷. Otro estudio, realizado por el Centro para la Lucha contra el Odio Digital (CCDH), reveló que se recomendaban vídeos de esta naturaleza incluso a usuarios menores de 18 años; bastaba con que mostraran interés por estos vídeos durante unos segundos⁸⁸.

Al basarse en parámetros destinados a la retención de usuarios, la denominada «neutralidad» de las recomendaciones personalizadas se traduce en un auténtico «sálvese quien pueda», en el que se ofrece

⁸⁷ GRIFFITHS, Scott et al. **¿Contribuye TikTok a los trastornos alimentarios? Una comparación de los algoritmos de TikTok de personas con trastornos alimentarios frente a un grupo de control sano.** Body Image, v. 51, p. 101807, 2024. DOI: 10.1016/j.bodyim.2024.101807. Disponible en: <<https://www.sciencedirect.com/science/article/pii/S1740144524001293>>. Consultado el: 17 de julio de 2025.

⁸⁸ CCDH. **«Deadly by Design»: TikTok introduce en los feeds de los usuarios contenido nocivo que promueve los trastornos alimentarios y las autolesiones.** Disponible en: <https://counterhate.com/wp-content/uploads/2022/12/CCDH-Deadly-by-Design_120922.pdf>. Consultado el 22 de septiembre de 2025



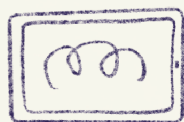
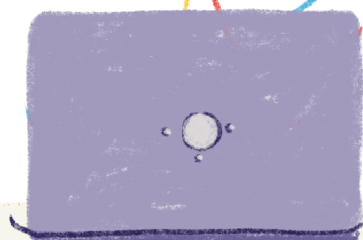
continuamente contenido inapropiado, que viola derechos y altamente sensible precisamente a aquellos usuarios que pueden verse más fácilmente seducidos por él; es decir, usuarios que ya presentan cierto grado de vulnerabilidad previa, que luego es explotada por los sistemas de recomendación.

Así, además de todos los daños para la salud mental de los niños y adolescentes relacionados con la adicción a las pantallas, los sistemas de recomendación algorítmica, basados en la lógica de captar la atención en todo momento, acaban agravando potencialmente los problemas de salud mental preexistentes y contribuyendo a que los niños y adolescentes que ya son vulnerables se vean cada vez más rodeados de estímulos inapropiados y nocivos. Para hacer frente a estos problemas, es necesario reconocer que la promoción de diferentes categorías de contenidos nocivos suele tener una raíz común: el diseño adictivo de las redes sociales y la incesante lucha por captar la atención de los usuarios menores de edad.

3.4.2. LOS IMPACTOS ESPECÍFICOS DE LOS SISTEMAS DE RECOMENDACIÓN ALGORÍTMICA EN LAS VIDAS Y LOS DERECHOS DE LOS NIÑOS Y ADOLESCENTES

Si la interacción con el diseño adictivo de las redes sociales es motivo de preocupación para todos sus usuarios, lo es aún más en el caso de los niños. Se trata, al fin y al cabo, de personas que atraviesan una etapa peculiar de desarrollo, marcada por la formación aún incompleta de la corteza prefrontal —la región del cerebro responsable del control inhibitorio, el control de los impulsos, el juicio, la resolución de problemas, la atención, la memoria y la toma de decisiones⁸⁹. Estas características de su etapa de desarrollo hacen que los niños y adolescentes sean especialmente susceptibles a desarrollar conductas impulsivas y a adquirir hábitos nocivos, lo que puede alterar su estructura cerebral y convertirse en prácticas que les acompañarán

⁸⁹ SOCIEDAD BRASILEÑA DE PEDIATRÍA (SBP). **#Menos Pantallas #Más Salud – Actualización 2024**. Río de Janeiro: SBP, 2024. Disponible en: https://www.sbp.com.br/fileadmin/user_upload/24604c-MO_MenosTelas_MaisSaude-Atualizacao.pdf. Consultado el 17 de julio de 2025.



durante el resto de sus vidas⁹⁰. No es casualidad que, según una encuesta realizada por Datafolha en septiembre de 2024, el 93 % de las familias brasileñas considere que los niños se están volviendo adictos a Internet⁹¹.

En la misma línea, el compendio elaborado por Unicef: «El cerebro adolescente: una segunda ventana de oportunidad» destaca que el cerebro adolescente es un trabajo «en curso» y señala los efectos negativos asociados al uso simultáneo de múltiples fuentes de información, como el deterioro de la memoria, el aumento de la impulsividad y la reducción del volumen en áreas importantes del cerebro, como la corteza cingulada anterior⁹². Esta región, en concreto, reviste gran importancia por ser la responsable de controlar y gestionar las emociones desagradables⁹³. Como consecuencia, resulta más difícil resistirse a la tentación de permanecer conectado a las redes, incluso cuando no se desea hacerlo.

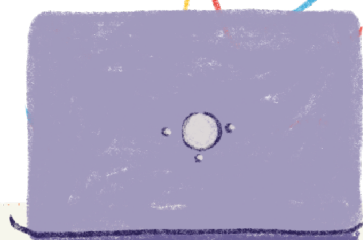
Teniendo en cuenta que, para el modelo de negocio de las grandes empresas tecnológicas, la participación equivale a beneficio, explotar las vulnerabilidades de los jóvenes ante estos patrones ocultos se convierte en una práctica ventajosa para los fines comerciales de las empresas. Estas prácticas explotadoras, sin embargo, contribuyen directamente al uso excesivo y problemático de las plataformas digitales, en contra de sus propios intereses y, a menudo, en contra de su propia voluntad.

⁹⁰ BRASIL. Secretaría de Comunicación Social de la Presidencia de la República. **Niños, adolescentes y pantallas: guía sobre el uso de dispositivos digitales**. Brasília, 2025. p. 31. Disponible en: <<https://www.gov.br/secom/pt-br/assuntos/uso-de-telas-por-criancas-e-adolescentes/guia>>. Consultado el: 14 de julio de 2025.

⁹¹ CAMPOS MELLO, Patrícia. **Las familias consideran que los menores de 14 años no deberían tener móvil ni acceder a las redes sociales**. Folha de S.Paulo, São Paulo, 11 de septiembre de 2024. Disponible en: <<https://www1.folha.uol.com.br/cotidiano/2024/09/familias-acham-que-filhos-com-menos-de-14-anos-nao-devem-ter-celular-nem-acessar-rede-social.shtml>>. Consultado el: 17 de julio de 2025.

⁹² UNICEF. **El cerebro adolescente: una segunda ventana de oportunidad**. Oficina de Investigación de UNICEF – Innocenti, 2017. 1 compendio. Florencia. ISBN 978-88-6522-048-1. p. 85.

⁹³ Stevens, F. L.; Hurley, R. A.; Taber, K. H. «Corteza cingulada anterior: un papel único en la cognición y la emoción». Journal of Neuropsychiatry and Clinical Neurosciences, vol. 23, n.º 2, págs. 121-125, primavera de 2011. DOI: 10.1176/jnp.23.2.jnp121



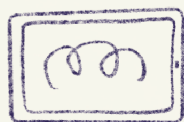
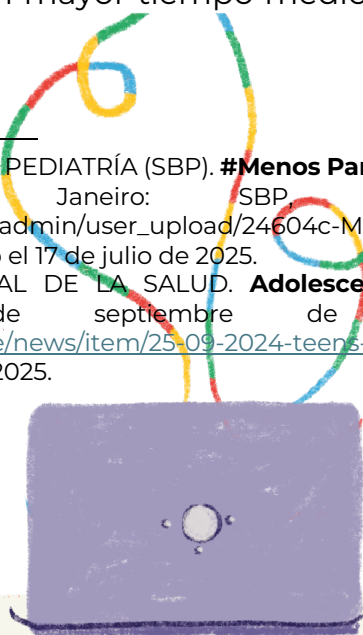
El diseño de las redes sociales se concibió para crear en los usuarios ciclos de recompensa variables similares a los de las máquinas tragaperras, lo que induce al uso compulsivo de estas aplicaciones para maximizar los beneficios de las empresas proveedoras. Este uso de técnicas de psicología conductual para maximizar la retención de usuarios tiene como primer (y quizás más evidente) efecto el fomento de un uso excesivo y problemático de las tecnologías digitales y el aumento del tiempo frente a las pantallas; de lo que se deriva una cascada de efectos secundarios para el desarrollo, la salud y el bienestar de los niños y adolescentes.

El uso de las tecnologías digitales se considera excesivo si supera el tiempo recomendado por la medicina para garantizar el equilibrio de dicho uso con otras actividades. En Brasil, la Sociedad Brasileña de Pediatría (SBP) recomienda que el contacto con las pantallas sea nulo para los niños menores de 2 años; que no supere 1 hora al día para los niños de entre 2 y 5 años; que sea inferior a 1 o 2 horas al día para los niños de entre 6 y 10 años; y que no supere las 2 o 3 horas al día para los adolescentes de entre 11 y 18 años⁹⁴. El término «uso problemático» ha sido utilizado por la Organización Mundial de la Salud (OMS) para referirse a patrones de uso de las tecnologías que adquieren características de compulsión⁹⁵.

La incorporación de patrones de diseño adictivos y técnicas de retención de usuarios en la arquitectura de las redes sociales va en una dirección diametralmente opuesta a la de limitar el uso de las pantallas de los dispositivos digitales para un uso saludable o no problemático. En América Latina, los efectos de esta incorporación han sido especialmente notables: hay estudios que muestran que, de los cinco países del mundo con mayor tiempo medio de uso diario de Internet,

⁹⁴ SOCIEDAD BRASILEÑA DE PEDIATRÍA (SBP). **#Menos Pantallas #Más Salud – Actualización 2024**. Río de Janeiro: SBP, 2024. Disponible en: <https://www.sbp.com.br/fileadmin/user_upload/24604c-MO__MenosTelas__MaisSaude-Atualizacao.pdf>. Consultado el 17 de julio de 2025.

⁹⁵ ORGANIZACIÓN MUNDIAL DE LA SALUD. **Adolescentes, pantallas y salud mental**. Copenhague, 25 de septiembre de 2024. Disponible en: <<https://www.who.int/europe/news/item/25-09-2024-teens--screens-and-mental-health>>. Consultado el: 17 de julio de 2025.



tres de ellos se encuentran en América Latina: Brasil (10:08 horas al día); Colombia (10:07 horas al día) y Argentina (9:39 horas al día).⁹⁶

En lo que respecta más concretamente a Brasil, diversos datos corroboran la percepción de que la difusión de modelos de negocio orientados a captar la atención ha dado lugar a un escenario de uso excesivo y problemático de las tecnologías digitales entre la población más joven. Un estudio que tenía como objetivo trazar un perfil del uso de pantallas entre las adolescentes del país llegó a conclusiones muy preocupantes en lo que respecta al uso excesivo de pantallas y dispositivos digitales. De las 214 adolescentes entrevistadas, con una edad media de 14,9 años, el 76,4 % utilizaba el móvil a diario durante más de 4 horas, mientras que el 25 % afirmó que lo utilizaba más de 9 horas al día.⁹⁷

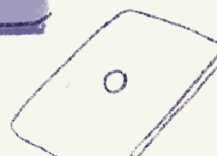
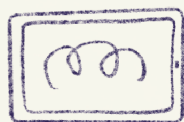
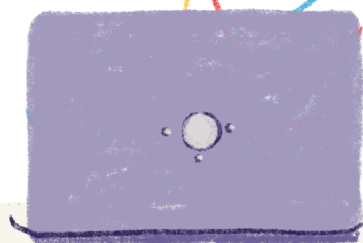
Este escenario de uso excesivo e incontrolado de las tecnologías digitales, tal y como señala la ciencia, resulta absolutamente devastador para los niños y adolescentes, con efectos que ni siquiera se conocen lo suficiente como para medir con precisión cómo se reflejarán y perdurarán en la vida adulta, ya que se trata de la primera generación de niños y adolescentes afectados por patrones de diseño adictivos. Sin embargo, existen pruebas de cómo se han ido materializando estos efectos, lo que se suma al conocimiento ya consolidado sobre el inmenso impacto que tienen las experiencias de la infancia y la adolescencia en el futuro de las personas⁹⁸.

Entre los niños en la primera infancia, el contacto prolongado con las pantallas y las tecnologías digitales se ha asociado a diversas alteraciones en su desarrollo psicomotor y psicosocial, entre ellas retrasos en el desarrollo del lenguaje y en el desarrollo cognitivo. Según una revisión sistemática de la bibliografía pertinente sobre el tema,

⁹⁶Feel Good Contacts. (2024). *Tiempo de pantalla por países: las naciones más pegadas a sus dispositivos*. <https://www.feelgoodcontacts.com/screen-time-countries>

⁹⁷ BENETTI, Webert Alex dos Santos; GOMES, Tcharles da Silva; BERMÚDEZ, Beatriz Elizabeth Bagatin Veleda. **Uso de pantallas por parte de las adolescentes en Brasil: prácticas y percepciones**. Revista Panamericana de Salud Pública, v. 49, e17, 2025. DOI: 10.26633/RPSP.2025.17. Disponible en: <https://pmc.ncbi.nlm.nih.gov/articles/PMC12007384/>. Consultado el 17 de julio de 2025.

⁹⁸Véase, por ejemplo: <https://ncpi.org.br/wp-content/uploads/2024/08/Impactos-da-desigualdade-na-primeira-infancia.pdf>. Consultado el 22 de septiembre de 2025.

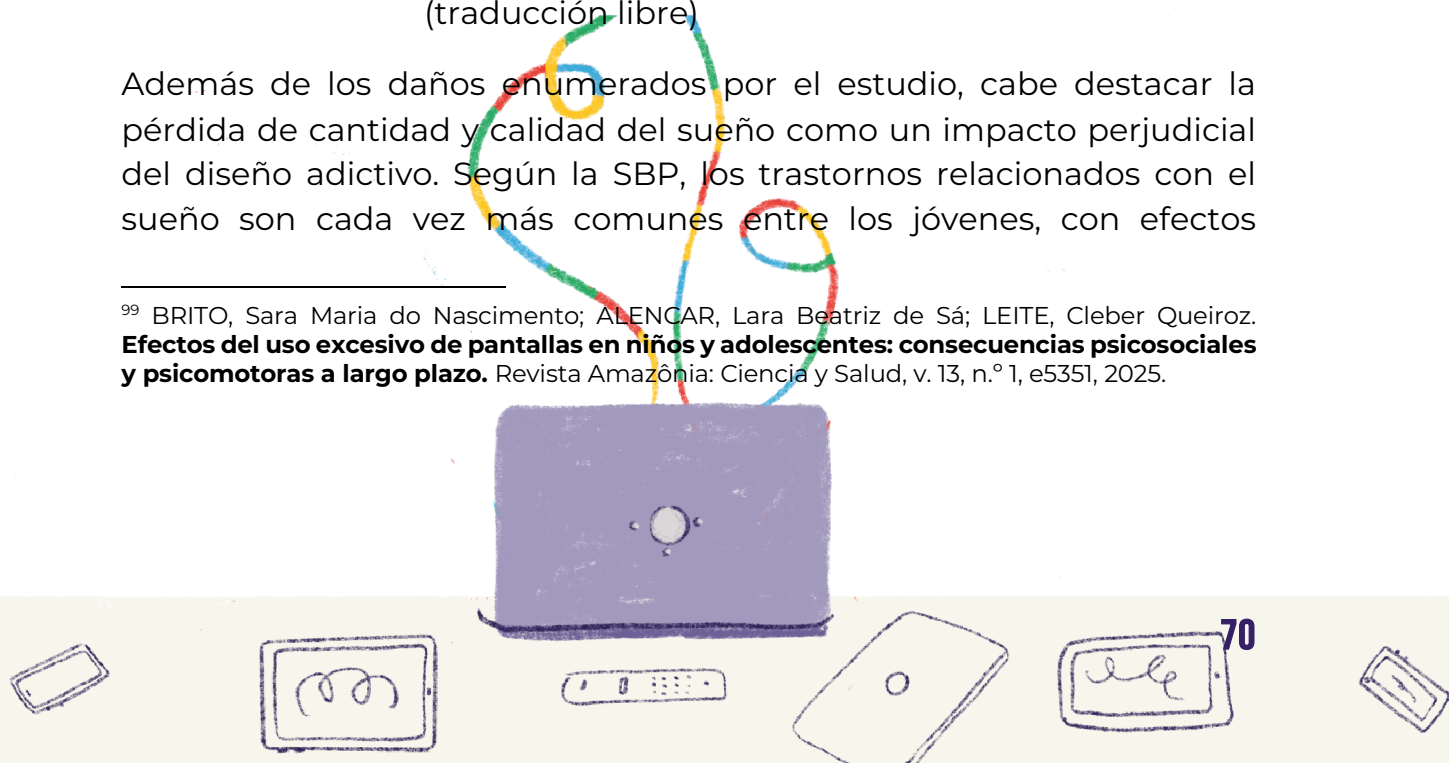


realizada por investigadores de la Facultad de Educación Superior de la Amazonia Reunificada (FESAR), todos los artículos analizados (12/12) apuntaban a la existencia de estas alteraciones, cuyos impactos son bastante amplios:

La exposición intensa al uso de pantallas en la primera infancia, entre los 0 y los 6 años de edad, se asocia con un mayor deterioro del desarrollo psicosocial y psicomotor de los niños. En cuanto a las consecuencias psicosociales, destacan los trastornos de la interacción social, los problemas en los ámbitos del lenguaje —especialmente el retraso en el habla—, la disminución de la calidad de los vínculos afectivos y las implicaciones negativas en el proceso de desarrollo de la regulación emocional. (...) Las consecuencias psicomotoras incluyen limitaciones en actividades que requieren habilidades motoras finas, debido a una menor interacción con juguetes físicos, un nivel reducido de actividad física, inestabilidad postural y dificultades en la percepción espacial, que integra la comprensión del espacio y el movimiento. La interacción temprana y el uso excesivo de los medios de comunicación también tienen un impacto negativo en el desarrollo neuropsicomotor de los niños, provocando retrasos motores, trastornos del sueño, cambios de comportamiento, problemas relacionados con una alimentación saludable, dificultades de atención y déficits en la interacción social y la cognición».⁹⁹ (traducción libre)

Además de los daños enumerados por el estudio, cabe destacar la pérdida de cantidad y calidad del sueño como un impacto perjudicial del diseño adictivo. Según la SBP, los trastornos relacionados con el sueño son cada vez más comunes entre los jóvenes, con efectos

⁹⁹ BRITO, Sara Maria do Nascimento; ALENCAR, Lara Beatriz de Sá; LEITE, Cleber Queiroz. **Efectos del uso excesivo de pantallas en niños y adolescentes: consecuencias psicosociales y psicomotoras a largo plazo.** Revista Amazônia: Ciência y Salud, v. 13, n.º 1, e5351, 2025.



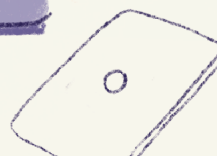
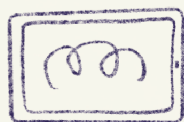
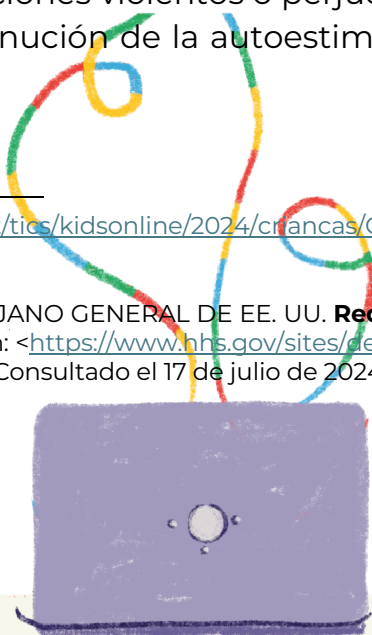
perjudiciales para su salud física y mental. Y esto no ocurre por casualidad: según la encuesta Tic Kids Online Brasil 2024, el 15 % de los niños y adolescentes brasileños de entre 9 y 17 años declararon que habían dejado de dormir porque pasaban demasiado tiempo con el móvil¹⁰⁰. En el estudio mencionado anteriormente sobre el uso de pantallas entre las adolescentes, el 44,2 % de ellas afirmaron que prolongaban el uso del móvil hasta el amanecer.

La SBP explica que la luz azul que emiten las pantallas de los dispositivos electrónicos afecta a la producción de melatonina del organismo y dificulta no solo conciliar el sueño, sino también mantener un sueño profundo y reparador de buena calidad. Esto provoca un aumento de la somnolencia diurna, problemas de memoria y una menor concentración durante el aprendizaje, y puede ser un factor que contribuya al desarrollo de síntomas de trastornos por déficit de atención e hiperactividad. Además, junto con otros daños causados por el uso excesivo y problemático de las redes sociales, la pérdida de sueño es un elemento que contribuye a crear un escenario de agravamiento de los riesgos para la salud mental de los niños y adolescentes que utilizan aplicaciones como TikTok.

En mayo de 2023, la máxima autoridad sanitaria de Estados Unidos, la Oficina del Cirujano General de EE. UU., emitió una alerta urgente de salud pública sobre los efectos en la salud mental y el bienestar de los niños y adolescentes causados por el uso de las redes sociales¹⁰¹. Según el informe, los jóvenes que pasan más de tres horas al día en las redes sociales se enfrentan al doble de riesgo de desarrollar problemas de salud mental, incluidos síntomas graves como la depresión y la ansiedad. Otros riesgos identificados incluyen una elevada exposición a contenidos e interacciones violentos o perjudiciales, capaces de causar daños como la disminución de la autoestima, efectos negativos sobre

¹⁰⁰ Véase: <<https://cetic.br/pt/tics/kidsonline/2024/crianças/G17/>>. Consultado el 29 de octubre de 2025

¹⁰¹ ADVERTENCIA DEL CIRUJANO GENERAL DE EE. UU. **Redes sociales y salud mental de los jóvenes.** 2023. Disponible en: <<https://www.hhs.gov/sites/default/files/sq-youth-mental-health-social-media-advisory.pdf>>. Consultado el 17 de julio de 2024.



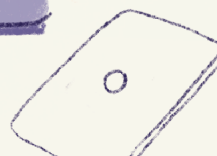
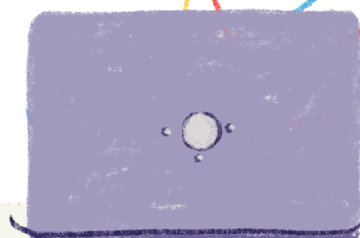
el sueño y la autoimagen, la normalización de actos de autolesión y las ideas suicidas.

Más recientemente, investigadores de la Universidad de Cornell publicaron un estudio que se propuso analizar los efectos de las redes sociales en la salud mental de los adolescentes durante cuatro años. A partir de este análisis, se concluyó que el 31,3 % de los 4 285 adolescentes estudiados presentaba patrones de uso de las redes sociales que tendían cada vez más a la adicción, y que estos mismos adolescentes tenían un mayor riesgo de desarrollar conductas suicidas en comparación con los demás.¹⁰²

En la misma línea, el informe «Driven Into the Darkness: How TikTok's 'For You' Feed Encourages Self-Harm and Suicidal Ideation» (Empujados a la oscuridad: cómo la sección «Para ti» de TikTok fomenta las autolesiones y las ideas suicidas), de Amnistía Internacional, muestra que los contenidos nocivos recomendados por los sistemas algorítmicos de TikTok agravan aún más el daño que la plataforma genera en la salud mental de los niños y adolescentes. Los testimonios de más de 300 niños, adolescentes y jóvenes escuchados en los grupos de discusión organizados por Amnistía Internacional son muy contundentes en este sentido, ya que muestran que la recomendación de vídeos guiada por la lógica de la retención de la atención tiene efectos muy graves, especialmente para los usuarios que ya padecen problemas de salud mental previos:

Varios jóvenes que declararon tener problemas de salud mental contaron a los investigadores de Amnistía Internacional sus experiencias al verse arrastrados por los «agujeros de conejo» de TikTok, es decir, contenidos desencadenantes y relacionados con la salud mental. Consideraban que la amplificación por parte de TikTok de contenidos problemáticos relacionados con la salud mental

¹⁰² XIAO, Yunyu et al. **A. Trayectorias de uso adictivo de las pantallas y conductas suicidas, ideas suicidas y salud mental en los jóvenes estadounidenses.** JAMA, DOI:10.1001/jama.2025.0109. Disponible en: <<https://jamanetwork.com/journals/jama/article-abstract/2835481>>. Consultado el 17 de julio de 2025.

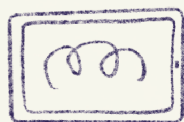
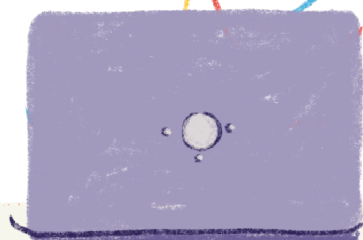


contribuía a exacerbar sus síntomas. Por ejemplo, «Luis», un estudiante universitario de Manila al que se le había diagnosticado un trastorno bipolar, describió su experiencia con la sección «Para ti» de TikTok: «Cuando me sentía deprimido, creo que el 80 % [del contenido] estaba relacionado con la salud mental. Es como una espiral. Es un agujero negro porque empieza con un solo vídeo. Si un vídeo consigue llamar tu atención, aunque no te guste, te lo vuelve a mostrar la próxima vez que abras TikTok y, como te resulta familiar, lo vuelves a ver, y luego lo vuelves a ver, y entonces la frecuencia con la que aparece en tu feed aumenta exponencialmente».

Haciéndose eco de la experiencia de otras personas, «Luis» describió cómo los periodos en los que se exponía deliberadamente a vídeos de TikTok que reflejaban sus propios pensamientos depresivos o de ansiedad le mantenían atrapado en bucles de contenido negativo incluso después de que la fase depresiva hubiera remitido:

«TikTok da por hecho que quieres este contenido concreto durante un periodo de tiempo determinado. Pero el caso es que, en mi caso, mis preferencias de contenido cambian mucho. Por ejemplo, un día estoy muy ansioso y quiero este tipo de contenido. Y otro día estoy muy feliz y entusiasmado con algo. Pero el problema es que sigo viendo contenido que es muy triste y deprimente, y eso me afecta mucho».

En Brasil, varios estudios indican que el impacto de las redes sociales en la vida de los niños y adolescentes se ha traducido en graves problemas para su salud mental. Según el Panorama de Salud Mental 2024, realizado por el Instituto Cactus en colaboración con AtlasIntel, el 15 % de los jóvenes de entre 16 y 24 años declaró que el uso de las redes sociales tenía un impacto muy negativo en su salud mental, lo que



apunta a correlaciones negativas entre la pérdida de control sobre el tiempo dedicado a las redes y los indicadores de salud mental¹⁰³. En la edición anterior del estudio, también se constató que el 43,5 % de los encuestados con un diagnóstico de ansiedad afirmaba pasar tres horas o más al día en las redes sociales.

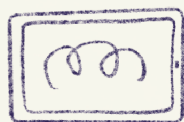
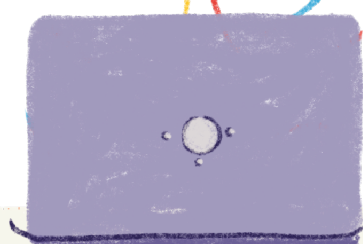
En la misma línea, los datos relacionados con la Red de Atención Psicosocial (RAPS) del Sistema Único de Salud (SUS), recopilados por el periódico Folha de S. Paulo, apuntan a un gran aumento de los casos de trastornos de ansiedad durante la adolescencia, un fenómeno que los expertos relacionan con los cambios culturales y de comportamiento de la última década, como el uso de las redes sociales¹⁰⁴. El psiquiatra Guilherme Polanczyk, de la Universidad de São Paulo (USP), añade que la pandemia ha contribuido a intensificar un proceso ya en marcha, caracterizado por una mayor exposición a las redes sociales con mecanismos adictivos y por la fragilidad emocional de una generación aún en formación.

Esto es precisamente lo que se desprende del gráfico elaborado a partir de los datos facilitados por RAPS: el aumento de los trastornos de salud mental entre los jóvenes es visiblemente más pronunciado desde el inicio de la pandemia, coincidiendo con el periodo de intensificación del uso de las redes sociales¹⁰⁵. Esta correlación refuerza la advertencia de los expertos sobre la relación entre el consumo excesivo de contenidos en las redes sociales —que explotan mecanismos de recompensa instantánea— y el agravamiento de la ansiedad, la depresión y otros

¹⁰³Instituto Cactus. (6 de noviembre de 2024). *Panorama de la salud mental: el 45 % de los encuestados considera que las redes sociales afectan negativamente al bienestar psicológico*. <https://institutocactus.org.br/panorama-da-saude-mental-terceira-coleta/>

¹⁰⁴FOLHA DE SÃO PAULO. **Los casos de ansiedad entre niños y jóvenes superan por primera vez a los de los adultos**. Folha Teen, 2024. Disponible en: < <https://www1.folha.uol.com.br/fohateen/2024/05/registros-de-ansiedade-entre-criancas-e-jovens-superam-os-de-adultos-pela-1a-vez.shtml> >. Consultado el 15 de octubre de 2025

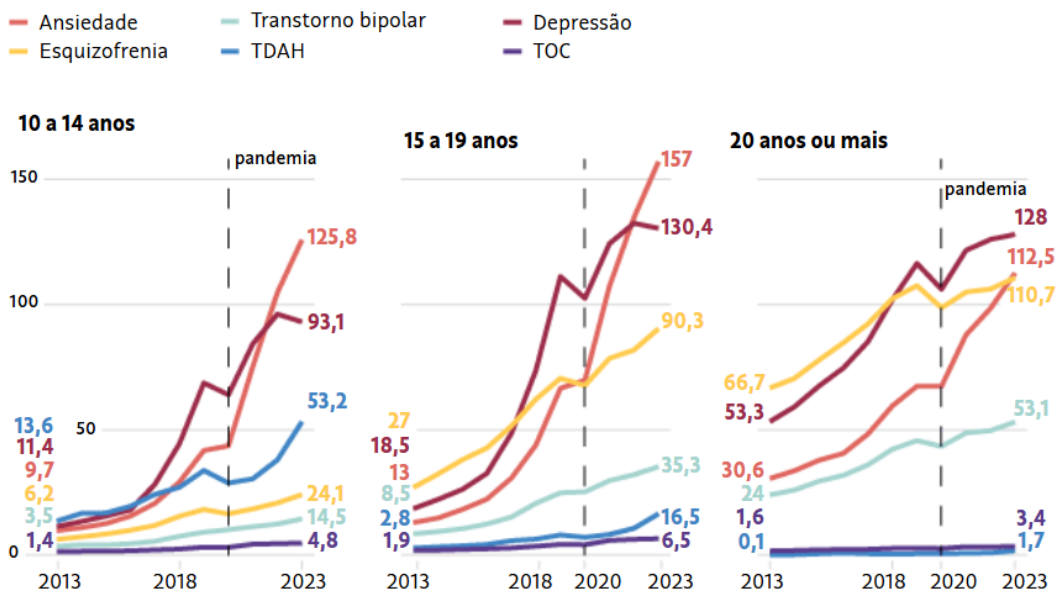
¹⁰⁵FACULTAD DE MEDICINA DE LA UFMG. **Salud de los estudiantes: el uso de pantallas en la adolescencia aumentó más de un 240 % durante la pandemia**. 8 de agosto de 2022. Disponible en: < <https://www.medicina.ufmg.br/saude-dos-estudantes-pesquisa-aponta-que-uso-de-telas-na-adolescencia-aumentou-mais-de-240-na-pandemia/> >. Consultado el 15 de octubre de 2025.



trastornos psicológicos entre niños y adolescentes.

Pacientes atendidos pelo SUS, para transtornos selecionados

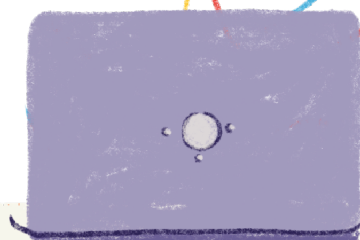
Taxa por 100 mil pessoas daquela faixa etária



Fonte: RAPS (Rede de Atenção Psicossocial) via Sistema de Informações Ambulatoriais/SUS

Aunque datos como estos merecen una atención urgente, conviene destacar que los casos de suicidio, depresión y trastornos mentales graves representan solo la parte más sensible y grave de las pérdidas más amplias que el modelo de negocio de las redes sociales genera en los niños y adolescentes. En otras palabras, incluso en el caso de aquellos niños que no reciben un diagnóstico de trastorno de salud mental, las prácticas relacionadas con la incorporación de mecanismos de diseño adictivo deben considerarse inapropiadas, perjudiciales y abusivas, ya que no solo se aprovechan de las vulnerabilidades propias de la etapa de desarrollo de estas personas, sino que también les privan de la autonomía para disfrutar de un bien que es absolutamente precioso para ellos, pero también escaso: el tiempo mismo.

Cabe destacar, una vez más, que la infancia y la adolescencia son períodos absolutamente cruciales de la experiencia humana, en los que la neuroplasticidad es más acusada y las experiencias vividas pueden dejar huellas profundas que acompañarán a las personas durante el resto de sus vidas. Al estar marcado por particularidades biológicas,

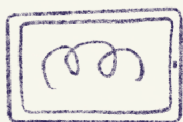
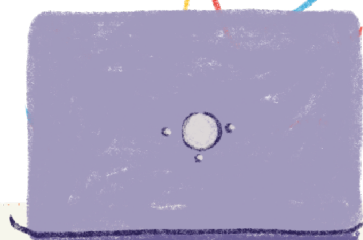


relacionadas con el desarrollo físico y neurológico, se trata de un período de la vida con contornos y límites objetivos: durante la vida adulta, el cerebro humano no tiene la misma capacidad de adaptación y asimilación que durante los primeros años de vida; por lo tanto, las oportunidades de desarrollo y aprendizaje que se tienen en este período difícilmente pueden reproducirse en momentos posteriores. Por esta razón, es necesario valorar el tiempo de la infancia y la adolescencia, llenándolo de experiencias que contribuyan, en la medida de lo posible, a la plena vivencia de esta etapa concreta de la vida humana. A los niños y adolescentes se les debe dar tiempo para jugar libremente, para recibir afecto, para el contacto con la naturaleza, para el estudio, para el descanso y para el ocio.

Al analizar la cuestión desde esta perspectiva, resulta evidente que las tácticas empleadas por las redes sociales para crear adicción en sus usuarios y maximizar el tiempo que pasan frente a las pantallas generan repercusiones que van más allá de la creación de un entorno propicio para la proliferación de trastornos de salud mental y contenidos nocivos. El tiempo que se pasa frente a las pantallas reduce el tiempo disponible para otras actividades que son esenciales para el desarrollo saludable e integral de los jóvenes y para que disfruten plenamente de su infancia y adolescencia; y, lo que es peor, las técnicas de diseño persuasivo privan a los niños y adolescentes de la autonomía sobre la gestión de su tiempo. Para comprender el alcance de estas pérdidas, resultan útiles los siguientes datos recopilados por la edición de 2024 de la encuesta Tic Kids Online Brasil¹⁰⁶ :

- (i) el 15 % de los niños y adolescentes entrevistados dejó de comer o de dormir a causa de Internet;
- (ii) el 16 % se sintió mal en algún momento por no poder conectarse a Internet;
- (iii) el 22 % se ha encontrado navegando por Internet sin estar realmente interesado en lo que veía;

¹⁰⁶ Véase: <<https://cetic.br/pt/tics/kidsonline/2024/criancas/G17/>>. Consultado el 29 de octubre de 2025



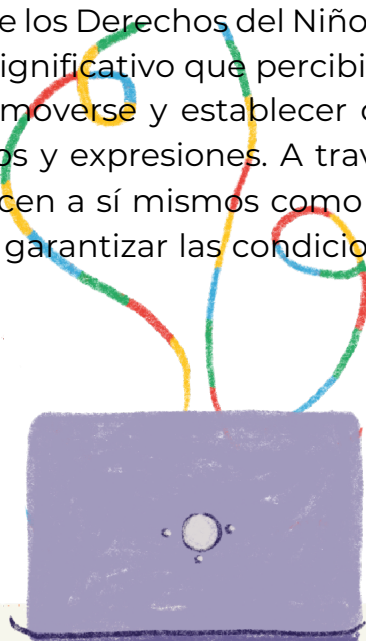
(iv) el 22 % dedicaba menos tiempo del que debería a la familia, a los amigos o a hacer los deberes porque pasaba demasiado tiempo en Internet;

(v) el 24 % afirmó que había intentado pasar menos tiempo en Internet, pero no lo había conseguido.

Los datos muestran que la pérdida de control sobre el tiempo de uso de Internet ya afecta a amplios sectores de la población de entre 9 y 17 años, lo que refleja patrones de adicción en el uso de la tecnología (uso problemático) y alteraciones en las actividades cotidianas. De ellos se desprende que el uso de Internet ha supuesto un perjuicio para otras actividades esenciales para los niños y adolescentes, como el tiempo de sueño y el tiempo con amigos y familiares, así como que este uso excesivo se produce en contra de la voluntad de los usuarios más jóvenes de las tecnologías digitales: casi una cuarta parte de los cuatro niños y adolescentes entrevistados afirmaron que habían intentado pasar menos tiempo en Internet y no lo habían conseguido, lo que pone claramente de manifiesto la pérdida de control sobre el tiempo dedicado a las plataformas digitales entre los niños.

De este modo, el diseño adictivo puede poner en peligro el sueño, el tiempo dedicado a las comidas, la actividad física y las interacciones sociales de los niños y adolescentes, además de una de las actividades más cruciales para el desarrollo de cualquier niño: el juego.

El acto de jugar libremente, utilizando todo el cuerpo, especialmente con otros niños, reviste una enorme importancia durante la infancia, hasta el punto de haber sido consagrado como un derecho humano y fundamental garantizado por el artículo 31 de la Convención de las Naciones Unidas sobre los Derechos del Niño. En las primeras etapas de la vida, nada es más significativo que percibirse a uno mismo como un ser capaz de actuar, moverse y establecer contacto con los demás a través de movimientos y expresiones. A través del juego, los niños se expresan y se reconocen a sí mismos como seres naturales, sociales y culturales, por lo que garantizar las condiciones objetivas para que los



niños jueguen libremente es esencial para su e¹⁰⁷ o presente y futuro. Según la valoración de la educadora y documentalista Renata Meirelles, creadora de la iniciativa «Territorio del Juego»:

«Tenemos que creer en el juego. Creer que él mismo ya reúne todos los estímulos necesarios para que los niños se conviertan en adultos felices. Hay estudios que ya demuestran que los adultos que, de niños, recibieron muchos estímulos adicionales no necesariamente crecieron con todas las características de alguien plenamente adaptado y en sintonía con el mundo. Pero, por desgracia, seguimos sin creer en el poder del juego».¹⁰⁸

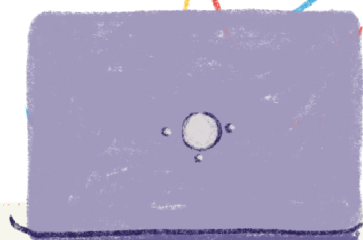
El juego es, por lo tanto, un espacio y una forma no solo de creación, sino también de construcción de la identidad de los niños. Es también un espacio para establecer vínculos duraderos con sus compañeros y comprender las dinámicas sociales. Como explica Jonathan Haidt, autor de «La generación ansiosa», el juego tiene la función de enseñar a los niños señales no verbales y límites para sus acciones, las cuales, cuando son incompatibles con las normas de convivencia ya incorporadas por otros niños, se reprimen en un entorno de bajo riesgo, donde cometer errores no tiene repercusiones significativas en el proceso de socialización¹⁰⁹. Para los niños, por lo tanto, jugar libremente con sus compañeros equivale a aprender, expresarse y desarrollarse.

Este juego corporal y relacional, tan esencial para la vida de los niños, no lo experimentan, sin embargo, mientras navegan por las redes sociales. Lo que ofrecen estas plataformas, por el contrario, es una forma de entretenimiento pasivo, desconectado del cuerpo y marcado, en muchas ocasiones, por contenidos perjudiciales para los niños. Es

¹⁰⁷ INSTITUTO ALANA. **En defensa del juego libre: una agenda para los Consejos Municipales de Educación.** São Paulo, 2022. Disponible en: <https://alana.org.br/wp-content/uploads/2022/11/direito-ao-brincar.pdf>. Consultado el 15 de octubre de 2025.

¹⁰⁸ TERRITORIO DEL JUEGO: **La importancia del juego: entrevista con Renata Meirelles y la esencia del juego.** Disponible en: <https://territoriodobrincar.com.br/territorio-do-brincar-na-midia/importancia-do-brincar-entrevista-com-renata-meirelles-e-a-essencia-da-brincadeira/>. Consultado el 22 de noviembre de 2025.

¹⁰⁹ HAIDT, Jonathan. **La generación ansiosa: cómo la infancia hiperconectada está provocando una epidemia de trastornos mentales.** 1.ª ed. São Paulo: Companhia das Letras, 2024. 440 p. ISBN 8535938532. Páginas 66 a 77.

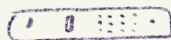
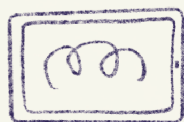
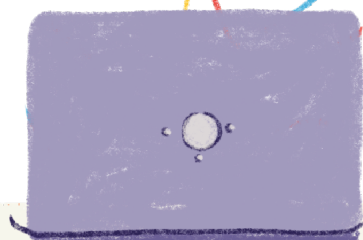


también un espacio en el que exponerse equivale a entrar en una lógica de autogestión, en la que se puede ser criticado al mismo tiempo por varios otros niños o adultos, lo que supone una pérdida irreparable para las necesidades de esta etapa de sus vidas. Para Haidt, las redes sociales son el espacio opuesto al juego. Y esta es también la razón por la que el uso prolongado de estas tecnologías, fomentado por técnicas de diseño persuasivo, priva a los niños de actividades que son esenciales para ellos. En palabras de Haidt:

«Aunque el contenido de estos sitios web podría filtrarse para eliminar material nocivo, el diseño adictivo de estas plataformas reduce el tiempo disponible para el juego presencial en el mundo real, hasta el punto de que podemos considerar que los smartphones y las tabletas, en manos de los niños, son un obstáculo para sus experiencias. Por supuesto, un smartphone abre las puertas a un mundo de nuevas experiencias, incluidos los juegos en línea (que son una forma de juego) y las relaciones a distancia. Sin embargo, el precio que hay que pagar por ello es la reducción del tipo de experiencia para la que los seres humanos han evolucionado y que necesitan en abundancia para convertirse en adultos socialmente funcionales. Es como si les diéramos a nuestros hijos iPads llenos de vídeos sobre cómo caminar, pero los vídeos fueran tan cautivadores que los niños nunca dedicaran el tiempo ni el esfuerzo necesarios para caminar de verdad».¹¹⁰

Las reflexiones de Haidt entablan un diálogo con las múltiples pérdidas descritas en la bibliografía relacionada con la disminución de las interacciones interpersonales provocada por el tiempo excesivo frente a la pantalla. Los trastornos de la interacción social, el deterioro de las habilidades lingüísticas —especialmente el retraso en el habla—, la

¹¹⁰ HAIDT, Jonathan. **La generación ansiosa: cómo la infancia hiperconectada está provocando una epidemia de trastornos mentales**. 1.ª ed. São Paulo: Companhia das Letras, 2024. 440 p. ISBN 8535938532. Página 69.



disminución de la calidad de los vínculos afectivos y las implicaciones negativas en el proceso de desarrollo de la regulación emocional, destacados por el estudio de revisión bibliográfica mencionado en este tema, están directamente relacionados con esta privación de interacción social en los primeros años de vida, ya que se refieren a habilidades que no pueden aprenderse sin el contacto directo con otras personas.

Incluso cuando los niños y adolescentes no están frente a las pantallas, su uso excesivo puede dar lugar a pérdidas en la experiencia plena y el disfrute de otras actividades, ya que este uso puede afectar negativamente a su capacidad de concentración. Las redes sociales basadas en la difusión de vídeos cortos resultan especialmente perjudiciales en este sentido: con la exposición continua a estos vídeos, el cerebro de los usuarios de estas plataformas se acostumbra a estímulos rápidos y sucesivos, perdiendo gradualmente la capacidad de asimilar información más densa o de mantener la atención en un mismo tema durante períodos de tiempo más prolongados. Por ello, varios estudios han demostrado correlaciones negativas entre el consumo de vídeos cortos y la motivación y el rendimiento académico¹¹¹

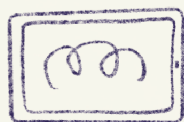
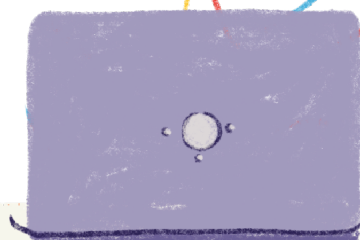
112 113

La pérdida de la capacidad para mantener la atención durante largos periodos de tiempo tiene graves implicaciones en varios ámbitos de la vida de los niños y adolescentes, además de en la educación. La capacidad de concentración es fundamental para la planificación, la resolución de problemas a largo plazo y la posibilidad de reflexionar y desarrollar un pensamiento crítico sobre la información con la que se

¹¹¹ LIAO, Mingyue. **Análisis de las causas, los mecanismos psicológicos y las consecuencias de la adicción a las redes sociales en China.** Frontiers in Psychology. 6 de agosto de 2024. Disponible en: <<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC11333346/>>. Consultado el 14 de julio de 2025.

¹¹² XIE, Jin, et al. **El efecto de la adicción a los vídeos cortos en la procrastinación académica de los estudiantes universitarios: un modelo de mediación moderada.** Frontiers in Psychology, Lausana, vol. 14, art. 1298361, 15 de diciembre de 2023. DOI: 10.3389/fpsyg.2023.1298361. Disponible en: <<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10756502/>>. Consultado el: 17 de julio de 2025.

¹¹³ YE, Jian Hong et al. **Efectos de la adicción a los vídeos cortos en la motivación y el bienestar de los estudiantes de formación profesional chinos.** Frontiers in Public Health, Lausana, vol. 10, art. 847672, 9 de mayo de 2022. DOI: 10.3389/fpubh.2022.847672. Disponible en: <<https://www.frontiersin.org/journals/public-health/articles/10.3389/fpubh.2022.847672/full>> Consultado el 17 de julio de 2025.



entra en contacto. También es una condición esencial para que las experiencias se vivan en toda su plenitud, con presencia y significado. Cuando esta capacidad se ve mermada, las experiencias tienden a volverse más superficiales y se reducen las posibilidades de actuar sobre el mundo y sobre lo que de él se percibe. «La vida se convierte en algo más pequeño de lo que podría ser», en palabras del escritor y activista Johann Hari.¹¹⁴

La cuestión que se plantea aquí, por lo tanto, va más allá de la protección de la salud mental de los niños y adolescentes: lo que está en juego es la preservación del tiempo de la infancia y la adolescencia, para que los niños y adolescentes puedan disfrutar libremente de esta etapa de sus vidas, realizando actividades que contribuyan a su bienestar y desarrollo integral, y sin verse atrapados por mecanismos adictivos de retención de la atención que, de forma insidiosa, no solo reducen el tiempo disponible para otras actividades, sino que también hacen que el tiempo de estas personas sea menos provechoso incluso cuando no están en contacto directo con las pantallas. Algunas organizaciones ya estiman que los niños y adolescentes de hoy en día pasarán 25 años de sus vidas desplazándose por la pantalla de sus teléfonos móviles.¹¹⁵ Esto debe interpretarse, en sí mismo, como un daño incalculable y una grave violación de sus derechos, que debe analizarse a la luz de las normas de protección de la infancia vigentes en el Derecho Internacional.

¹¹⁴ HARI, Johann. **Stolen Focus: Why can't you pay attention.** Traducido al portugués por Luis Reyes Gil. Pág. 21. 1.ª ed. Porto Alegre: Vestigio, 2023. 320 p. ISBN 978-6560020047.

¹¹⁵ SCRIPPS NEWS. **Un estudio advierte de que los estudiantes van camino de pasar 25 años de su vida pegados al móvil.** Disponible en: <<https://www.scrippsnews.com/science-and-tech/social-media/students-on-track-to-spend-25-years-of-their-lifetime-on-phones-study-warns>>. Consultado el 18 de julio de 2025.

