

Informe de investigación

NUEVAS TECNOLOGÍAS Y DERECHOS HUMANOS:

IMPACTOS, DESAFÍOS Y OPORTUNIDADES EN LA ERA DE LA CONECTIVIDAD DIGITAL

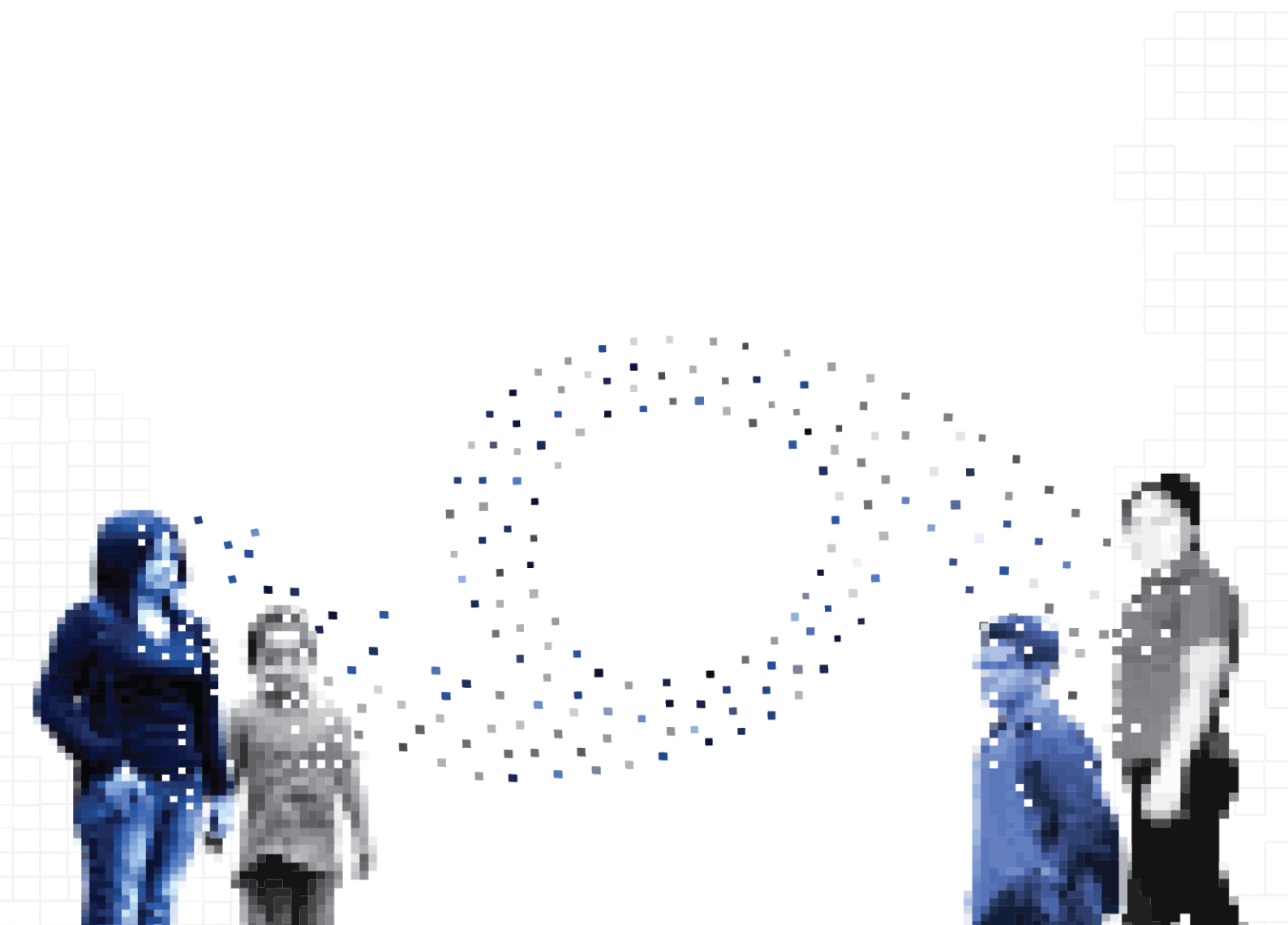


IDEHPUCP



KONRAD
ADENAUER
STIFTUNG

ESTADO DE DERECHO · LATINOAMÉRICA



Informe de investigación

NUEVAS TECNOLOGÍAS Y DERECHOS HUMANOS:

**IMPACTOS, DESAFÍOS Y OPORTUNIDADES
EN LA ERA DE LA CONECTIVIDAD DIGITAL**



IDEHPUCP



INFORME DE INVESTIGACIÓN
NUEVAS TECNOLOGÍAS Y DERECHOS HUMANOS:
IMPACTOS, DESAFÍOS Y OPORTUNIDADES EN LA ERA DE LA CONECTIVIDAD DIGITAL

FUNDACIÓN KONRAD ADENAUER
Programa de Estado de Derecho para Latinoamérica
Calle 93B No. 18-12, piso 7
Bogotá
República de Colombia
Tel.: (+57 1) 743 09 47
Fax: (+57 1) 743 09 47-7
www.kas.de/web/rspla
iusla@kas.de
Twitter: @KASiusLA
Facebook: www.facebook.com/kasiusla

© PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ, 2023
INSTITUTO DE DEMOCRACIA Y DERECHOS HUMANOS DE LA
PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ (IDEHPUCP)
Tomás Ramsey 925, Lima 17 - Perú
Tel.: (51 1) 626-2000, anexos: 7500 / 7501
ideh@pucp.edu.pe
www.idehpucp.pucp.edu.pe

Coordinadora de la publicación: Valeria Reyes
Autoras: Paola Miranda, Yazmine Ruiz y Daniela Pulido

Corrección de estilo: Rocío Reátegui
Diseño y diagramación: Ximena Barreto

Primera edición digital: diciembre 2023

Hecho el Depósito Legal en la Biblioteca Nacional del Perú N.º 202312102

ISBN: 978-612-4474-48-4

ÍNDICE

Siglas.....	4
Presentación.....	6
1. Introducción.....	8
2. Nuevas tecnologías y derechos humanos: algunos conceptos clave.....	9
3. Evolución del derecho internacional de los derechos humanos y su relación con las nuevas tecnologías.....	12
4. ¿Pueden las nuevas tecnologías socavar los derechos humanos?	
Análisis sobre escenarios de posibles amenazas.....	15
4.1. Amenazas a los derechos a la privacidad, libertad de expresión y participación política.....	16
4.1.1. Derecho a la privacidad.....	16
4.1.2. Libertad de expresión.....	19
4.1.3. Derecho a la participación política.....	22
4.2. Amenazas a los derechos a la salud, a la educación y al trabajo.....	25
4.2.1. Derecho a la salud.....	25
4.2.2. Derecho a la educación.....	28
4.2.3. Derecho al trabajo.....	31
5. La incorporación progresiva de las nuevas tecnologías en el derecho internacional de los derechos humanos.....	34
5.1. Sistema Universal de Derechos Humanos.....	34
5.1.1. Órganos de las Naciones Unidas.....	34
5.1.2. Órganos de los tratados.....	41
5.1.3. Procedimientos especiales.....	42
5.2. Sistemas Regionales de Derechos Humanos.....	45
5.2.1. Sistema Interamericano de Derechos Humanos.....	45
5.2.2. Sistema Europeo de Derechos Humanos.....	48
6. Buenas prácticas estatales y multilaterales para garantizar la protección de los derechos humanos en el contexto de las nuevas tecnologías.....	50
6.1. Buenas prácticas estatales.....	51
6.1.1. Medidas legislativas y políticas públicas.....	51
6.1.2. Jurisprudencia.....	56
6.1.3. Buenas prácticas multilaterales.....	60
7. Conclusiones y recomendaciones.....	65
8. Referencias.....	68

SIGLAS

ACNUDH	Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos
ADN	Ácido desoxirribonucleico
BCI (siglas en inglés)	Interfaz cerebro-computador
CADH	Convención Americana sobre Derechos Humanos
CDN	Convención sobre los Derechos del Niño
CEDH	Convenio Europeo de Derechos Humanos
CEPAL	Comisión Económica para América Latina y el Caribe
CIDH	Comisión Interamericana de Derechos Humanos
Comité DESC	Comité de Derechos Económicos, Sociales y Culturales
Convenio 108+	Convenio para la Protección de las Personas con respecto al Tratamiento de Datos Personales del Consejo de Europa
Corte IDH	Corte Interamericana de Derechos Humanos
DADDH	Declaración Americana de Derechos y Deberes del Hombre y el Ciudadano
DCP	Derechos civiles y políticos
DESC	Derechos Económicos, Sociales y Culturales
DIDH	Derecho Internacional de los Derechos Humanos
DUDH	Declaración Universal de Derechos Humanos
IA	Inteligencia artificial
INDECOPI	Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual
NNA	Niños, niñas y adolescentes
OEA	Organización de Estados Americanos
OIT	Organización Internacional del Trabajo
ONU	Organización de las Naciones Unidas
PIDESC	Pacto Internacional de Derechos Económicos, Sociales y Culturales
PIDCP	Pacto Internacional de DCP
Protocolo de San Salvador	Protocolo Adicional a la Convención Americana sobre Derechos Humanos en materia de Derechos Económicos, Sociales y Culturales
RELE	Relatoría para la Libertad de Expresión de la CIDH
SADH	Sistema Africano de Derechos Humanos
SEDH	Sistema Europeo de Derechos Humanos
SIDH	Sistema Interamericano de Derechos Humanos
SUDH	Sistema Universal de Derechos Humanos
STJUE	Sentencia del Tribunal de Justicia de la Unión Europea

TEDH	Tribunal Europeo de Derechos Humanos
TIC	Tecnologías de la Información y la Comunicación
UE	Unión Europea
UNESCO	Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura
UNICEF	Fondo de Naciones Unidas para la Infancia
URL	Uniform Resource Locator

PRESENTACIÓN

El desarrollo tecnológico, tanto en el ámbito estatal como privado, ha llevado a que la población —voluntariamente o no— se adapte a una realidad cambiante y a que fortalezca sobre la marcha nuevas habilidades para entenderla y ejercer en esta nueva esfera sus derechos sin que estos sean vulnerados.

En un espacio tan amplio, en donde ya no es fácil saber si estamos ante una persona real o bajo una maqueta virtual que, gracias a la inteligencia artificial, simula ser una persona, preocupa saber cómo se garantizará y promoverá el respeto y la plena garantía de los derechos humanos de quienes interactuamos en esta «dimensión tecnológica». Las fronteras ya no ayudan, al menos para procurar identificar si la persona responsable, por ejemplo, de un acto de espionaje virtual, puede ser investigada en un país en específico, bajo una legislación en concreto, y rendir declaración en el marco de un debido proceso.

La investigación judicial o la resolución de conflictos que gira alrededor de las nuevas tecnologías se torna entonces difícil de lograr. Asimismo, como parte de las garantías al debido proceso, la hoy denominada «carga dinámica de la prueba» o «inversión de la carga de la prueba», que puede recaer sobre actores económicos que desarrollan actividades tecnológicas, no necesariamente asociadas a una empresa formal, pone en riesgo una figura jurídica creada para determinar la responsabilidad jurídica. Ello en casos donde las personas que denuncian o demandan la violación de sus derechos no están en las mejores condiciones de probar sus alegatos al no tener evidencia científica necesaria para ello.

En el marco de la justicia, que involucra el dinamismo tecnológico en el «ecosistema digital», esto desentraña un desafío aún mayor: entender lo científico y combinar dicho conocimiento con lo jurídico para valorar si un hecho caracteriza una violación de los derechos humanos. En el marco de un Estado democrático de derecho, la democracia implica abordar estas complejidades tecnológicas de una manera sencilla y de la forma más comprensible posible para que el conocimiento no repose en unos cuantos, sino que siga su curso y fluya en el conocimiento jurídico para generar evidencia y resolver conflictos.

Así como la base científica es esencial, también es vital para nuestras democracias conocer qué derechos pueden ser vulnerados en estos espacios digitales y cuál es el sustento legal nacional y/o internacional. El Sistema Interamericano de Derechos Humanos, el Sistema de las Naciones Unidas y la experiencia comparada de diversos países a nivel nacional han delineado estándares jurídicos importantes sobre estos temas. Si viramos alrededor de nosotros en este momento, podemos comprender que para realizar nuestro trabajo diario usamos medios de comunicación masivos. La educación ha cambiado, las metodologías han evolucionado, y hoy en día es más fácil encontrar información; incluso delegar nuestro pensar a un ordenador, que en minutos puede resolver un problema. Las esferas de participación política tampoco han sido ajenas a este desarrollo, las famosas *fake news* pueden mover las cifras en horas en favor de una persona que postula a un cargo público. De la misma forma, nuestra intimidad se pone en riesgo, incluso sin pensarlo. Un computador, a través de algoritmos, puede saber cuáles son nuestras preferencias de ocio o profesionales.

Comprender estos estándares internacionales es posible gracias al estudio titulado *Nuevas tecnologías y derechos humanos* que presentamos el día de hoy, en el que el Instituto de Democracia y Derechos Humanos de la Pontificia Universidad Católica del Perú (IDEHPUCP), de una manera impecable, nos hace navegar a través del desarrollo de estándares internacionales no solo del Sistema Interamericano de Derechos Humanos, sino también de las Naciones Unidas y de tribunales regionales, como el europeo. El estudio tiene como base principalmente el

derecho a la salud, a la educación, al trabajo, a la participación política, a la libertad de expresión y a la privacidad.

Un aspecto relevante también de este estudio es el análisis de buenas prácticas a nivel estatal, mediante el cual se analizan los avances legislativos y en políticas públicas en diversos países de la Región sobre medios tecnológicos. La comparación con lo que sucede en el terreno —es decir, a nivel de los Estados— complementa perfectamente un análisis de estándares regionales de derechos humanos.

El Programa Estado de derecho para Latinoamérica de la Fundación Konrad Adenauer cuenta con una línea sobre el Sistema Interamericano de Derechos Humanos y otra sobre Empresas y Derechos Humanos. A través de ambas hemos ido acercándonos y desarrollando estudios que analicen el vínculo innegable entre las nuevas tecnologías y los derechos humanos. El IDEHPUCP ha sido clave en esta búsqueda académica para reflexionar de manera responsable sobre estas temáticas y avanzar hacia algo que es importante para nosotros, que es hacer democrático el conocimiento y que estos temas nuevos no se vuelvan entramados jurídicos difíciles de comprender.

Celebramos esta obra y esperamos que la puedan disfrutar y generar reflexiones clave para que sobre esta base se siga construyendo conocimiento acerca de las nuevas tecnologías y los derechos humanos, ámbitos en los que debemos tener como pilar central a las personas y el pleno respeto de su dignidad en sus entornos.

HARTMUT RANK

Director del Programa Estado de Derecho para Latinoamérica
Fundación Konrad Adenauer

MIGUEL BARBOZA LÓPEZ

Coordinador de Proyectos del Programa Estado de Derecho para Latinoamérica
Fundación Konrad Adenauer

1. INTRODUCCIÓN

Las nuevas tecnologías han llegado para revolucionar la concepción humana de la realidad. Aquellas miradas futuristas en las que se proyectaba un mundo que se volviera cada vez más funcional por su recurso a estas herramientas forman, en la actualidad, parte de lo cotidiano. Lo que se percibía como una ficción lejana, como la posibilidad de establecer comunicación inmediata e intercambiar información instantánea a pesar de las distancias remotas, conocer en tiempo real sucesos que ocurren en el espacio estelar, o interactuar con formas de inteligencia distintas a la humana, que permiten desde la atención automatizada al cliente hasta la conducción autónoma de vehículos, ocurre de manera diaria en las vidas de todos y todas.

Aunque las nuevas tecnologías ofrecen diversas virtudes para facilitar nuestras interacciones sociales, lo cierto es que su verdadero alcance e impacto en los distintos ámbitos de la vida humana es aún un terreno desconocido. Desde un enfoque utilitario, podría decirse que estas herramientas se encuentran al servicio de las personas, pero lo cierto es que existe en torno a ellas una presunción de neutralidad y objetividad que puede resultar en la invisibilización de algunas consecuencias nocivas derivadas de su uso. Lo anterior es particularmente preocupante cuando se analiza desde el enfoque del respeto y de la garantía de los derechos humanos.

En línea con esta preocupación, este informe surge de una pregunta clave y busca llegar a un norte claro: ¿la positivización e institucionalidad de los derechos humanos en su configuración actual resultan suficiente para guiar las acciones estatales frente a los retos que llegan con las nuevas tecnologías? Al responder a esta pregunta, se pretende también: a) describir las amenazas que supone el uso descontrolado de estas herramientas; b) delimitar las posibilidades de respuesta que el DIDH ofrece frente a este fenómeno; y c) echar luz sobre las oportunidades ofrecidas por las diversas medidas que de manera individual o coordinada vienen adoptando sobre el particular diversos Estados y organizaciones internacionales.

En vista de ello, este informe sigue la siguiente estructura: en primer lugar, se comparten con el lector algunos conceptos clave para que se familiarice con el tema de las nuevas tecnologías y los derechos humanos. En segundo lugar, se analiza la evolución del DIDH para determinar hasta qué punto la proliferación de estas tecnologías supone un giro en la concepción de esta disciplina como se le conoce hoy en día. En un tercer momento, se reflexiona sobre las potenciales amenazas que emergen respecto a los derechos humanos con el desarrollo de las nuevas tecnologías y se evalúan, de modo diferenciado, los impactos que estas pueden generar sobre el goce y disfrute de los derechos a la privacidad, la libertad de expresión, la participación política, la salud, la educación y el trabajo. Seguidamente, se presentan, en dos secciones, las respuestas que de modo inicial se han brindado tanto desde los órganos internacionales de protección de derechos humanos como desde los Estados y otros actores de la comunidad internacional para hacer frente a este desafío. Finalmente, se concluye con un apartado sobre la necesidad de transversalizar el enfoque del DIDH en la creación y el desarrollo de las nuevas tecnologías.

Ya en 1951, Marshall McLuhan vaticinaba la llegada del Internet como un medio que nos transformaría en una «aldea global» basada en una lógica de interdependencia y coexistencia (BBC Mundo, 2017). Al mismo tiempo, el filósofo canadiense alertaba sobre los peligros de supeditar a las personas al poder del Internet con el irremediable riesgo de que «no nos quede ningún derecho» (BBC Mundo, 2017). Esta investigación constituye un esfuerzo no solo por caracterizar el momento histórico que nos encontramos y describir cómo desde distintos frentes se vienen tomando medidas para conciliar los objetivos que se plantearon los Estados con respecto a los derechos humanos y las posibilidades infinitas de las nuevas tecnologías; sino que también pretende ser una contribución a una desafiante e inacabada discusión acerca de la reconfiguración del mundo como lo conocemos.

2. NUEVAS TECNOLOGÍAS Y DERECHOS HUMANOS: ALGUNOS CONCEPTOS CLAVE

En la actualidad, la aparición y propagación de nuevas tecnologías, tales como la IA y el Aprendizaje Automático o Machine Learning, han propiciado una transformación tan significativa en la economía y, en términos más generales, en los sistemas sociales, que inclusive hoy en día se ha empezado a discutir sobre el posible surgimiento de una Cuarta Revolución Industrial. Así, mientras que la Tercera Revolución Industrial comenzó en la década de 1950 con el desarrollo de la electrónica, las tecnologías de la información y la producción automatizada; la llamada «Cuarta Revolución Industrial» combinaría avances en diversas tecnologías digitales, como la IA, la automatización, el Internet de las cosas,¹ la analítica de datos, la computación en la nube y la robótica (Schwab, 2016, p. 7).

La palabra «revolución» denota un cambio abrupto y radical. De hecho, las revoluciones han ocurrido a lo largo de la historia cuando las nuevas tecnologías y nuevas formas de percibir el mundo desencadenan un cambio profundo en los sistemas económicos y las estructuras sociales (Schwab, 2016, p. 11). En el presente, el mundo está experimentando una transformación sustancial debido a los avances de las nuevas tecnologías, que aparecen intrínsecamente unidas a la idea de innovación o progreso indefinido al permitirle al ser humano realizar ciertas actividades de manera más eficiente, y con menor esfuerzo y riesgo (Díaz y Castro, 2021, p. 16). Cabe mencionar que lo «nuevo» no es la tecnología *per se*, sino la combinación e interacción de tecnologías, las cuales dan nacimiento a nuevos productos y servicios (UNESCO, 2001, párr. 1).

Las TIC y las nuevas tecnologías se encuentran vinculadas de forma muy cercana en la medida en que se complementan y potencian mutuamente. Mientras que las TIC constituyen aquel «conjunto variado de herramientas y recursos tecnológicos usados para transmitir, almacenar, crear, compartir o intercambiar información» (UNESCO, 2021a, p. 12); las nuevas tecnologías se refieren a avances tecnológicos innovadores y emergentes en diversas áreas, incluyendo la informática. Entre las TIC, destacan recursos tecnológicos como el «*software*, computadoras, Internet (sitios web, blogs y correos electrónicos), tecnologías de radiodifusión en directo (radio, televisión y difusión por Internet), tecnologías de radiodifusión grabada (podcasting, reproductores de audio y video, y dispositivos de almacenamiento) y telefonía (fija o móvil, satelital, visio/videoconferencia, etc.)» (UNESCO, 2021a, p. 12). Así, la infraestructura, la comunicación, la seguridad y la innovación en las TIC son fundamentales para el desarrollo, la implementación y la mejora de las nuevas tecnologías (Holtgrewe, 2014, p. 10).

Entre las TIC, la tecnología que más ha impulsado el desarrollo de nuevas tecnologías y que ha repercutido de manera definitiva en las dinámicas sociales de la mayor parte de la población a nivel mundial es el Internet. Como bien señala Castells, en realidad, el Internet es una tecnología antigua que se utilizó por primera vez en 1969, pero cuya difusión a gran escala tendría lugar hasta veinte años después por diversos factores; entre ellos, la propagación de los ordenadores personales, así como de programas de *software*² fáciles de usar y que, por ende, simplificaban la descarga, el acceso y la transmisión de contenido (2009, p. 97). Inicialmente, el Internet se concibió como un sistema mundial de redes informáticas que permitía que millones de computadoras se comunicaran entre sí (Glowniak, 1995, p. 60).

¹ El Internet de las cosas (IoT) es «una infraestructura global que permite servicios avanzados mediante la interconexión de cosas (físicas y digitales) sobre la base de tecnologías de la información y las comunicaciones interoperables existentes y en evolución» (UNESCO, 2021a).

² «Los dispositivos tecnológicos como computadores o smartphones están compuestos por *hardware* y *software*. *Hardware* es el conjunto de componentes físicos de los que está hecho el equipo y *software* es el conjunto de programas o aplicaciones, instrucciones y reglas informáticas que hacen posible el funcionamiento del equipo» (GCF Global, s/f).

No obstante, la anterior definición ha ido ampliándose a fin de mantenerse al día con la propia evolución de la tecnología. Hoy en día, el Internet no solo les permite a las computadoras acceder a una multiplicidad de contenidos a través de la World Wide Web (WWW),³ sino que otros dispositivos electrónicos —por ejemplo, los *smartphones*, las *laptops* y *tablets*, los televisores e incluso los relojes inteligentes— son capaces de acceder a miles de millones de documentos digitales a través del uso de navegadores web como Chrome, Safari, Microsoft Edge, Firefox, entre otros (Gil, 2020).

Hoy en día, el Internet es indesligable de las nuevas tecnologías, pues actúa como una plataforma fundamental que permite que se implementen y funcionen muchas de estas. Por ejemplo, los algoritmos, la IA y la analítica de datos (también conocido como Big Data) se basan en gran medida en la conectividad a Internet para recopilar, transmitir y procesar datos. A continuación, se presenta una breve definición y explicación sobre el funcionamiento y las implicancias de los algoritmos, la IA (incluido el Machine Learning) y la analítica de datos o Big Data.

TABLA 1. CONCEPTOS CLAVE SOBRE NUEVAS TECNOLOGÍAS

ALGORITMOS	Los algoritmos pueden definirse como aquellos procesos o conjuntos de reglas que se han de seguir para resolver problemas o realizar tareas (Sales, 2021).
IA	<p>Si bien no existe una única definición de IA, esta puede describirse como aquel «conjunto de TIC avanzadas que permiten el funcionamiento de máquinas capaces de imitar ciertas funcionalidades de la inteligencia humana, incluidas características como la percepción, el aprendizaje, el razonamiento, la resolución de problemas, la interacción mediante el lenguaje y hasta la producción de trabajo creativo» (UNESCO, 2021a).</p> <p>El Machine Learning es una subcategoría de la IA que se centra en el desarrollo de algoritmos y modelos que permiten a las computadoras aprender y tomar decisiones basadas en grandes volúmenes de datos o Big Data (Columbia Engineering, s/f). El término «Big Data» hace alusión a grandes cantidades de datos estructurados y no estructurados que se generan todos los días y que pueden provenir de distintas fuentes, incluidas las redes sociales, sensores, etc. El Machine Learning y el Big Data se encuentran estrechamente entrelazados, pues es imposible implementar el primero sin acceder a grandes cantidades de datos. La razón de ello es que los algoritmos de Machine Learning requieren una cantidad significativa de datos para aprender y mejorar su rendimiento (Britts Imperial University College, 2023).</p> <p>Existen dos categorías principales de algoritmos de Machine Learning: supervisados y no supervisados. Los primeros implican «enseñar» a la máquina a producir resultados basados en sus datos de entrenamiento, que ya están etiquetados o estructurados. En cambio, los segundos funcionan con datos no estructurados, es decir, datos que aún no han sido clasificados o etiquetados (Sarker, 2021, pp. 3-4).</p>

³ La WWW es una de las formas en que se comparte información en Internet (otras incluyen el correo electrónico, el protocolo de transferencia de archivos y los servicios de mensajería instantánea). A modo de analogía, puede pensarse en el Internet como una librería, y en los sitios *web* como los libros, revistas, periódicos, audiolibros, etc., que se encuentran dentro de esta (Gil, 2020).

Big Data	Se trata de un término para hacer referencia a grandes cantidades de datos o información digital cuya cuantía hace imposible (al menos con la capacidad humana actual) procesar o clasificar la información suministrada (Asquerino, 2022, p. 338). Para procesar e interpretar dichos datos (los cuales pueden ser de diversa índole: texto, imagen, video o sonido), se requerirán equipos de cómputo de alto rendimiento, así como programas o técnicas de análisis especializadas (Téllez, 2020, pp. 157-158). Finalmente, los datos recabados son almacenados y procesados tanto por agentes gubernamentales como por compañías privadas del rubro de la tecnología e información como Meta, Google, Amazon, Uber, etc. (Ureña, 2019, p. 100).
Biometría	Definida como la ciencia de la identificación de los seres humanos sobre la base de características físicas únicas (Ruiz, Rodríguez y Olivares, 2009, p. 30). El término «biometría» se ha utilizado para aludir a «los métodos automáticos que analizan determinadas características humanas con el fin de identificar y autenticar a las personas» (Tapiador, 2005, p. 56). Según Privacy International (2013), durante las últimas décadas, diversos países alrededor del mundo han adoptado esta tecnología con diversos fines: planes de identificación universal de la población, la realización de procesos electorales o la facilitación de servicios básicos y asistenciales.
Neurotecnologías	Las neurotecnologías han sido referidas como aquellos «sistemas e instrumentos que establecen una vía de conexión con el cerebro humano y que pueden registrar, leer y aumentar las capacidades cerebrales» (Orias, 2022, pp. 213-2014). En las últimas décadas, las neurotecnologías han tenido avances notables. Por ejemplo, «los implantes para la estimulación eléctrica de áreas profundas del cerebro se usan rutinariamente para el tratamiento de trastornos motores como el Parkinson y la distonía» (Fuentes, 2021).

Si bien la lista de nuevas tecnologías es bastante extensa, las definiciones presentadas hasta el momento se han seleccionado con el objetivo de permitir un adecuado entendimiento de las principales discusiones desarrolladas en este estudio, las cuales se relacionan con los retos y las oportunidades que las nuevas tecnologías representan en el ámbito de los DCP (derechos a la privacidad, libertad de expresión y participación política), así como de los DESC (derechos a la salud, educación y trabajo), conforme se desarrolla en la sección 4 del presente informe.

3. EVOLUCIÓN DEL DERECHO INTERNACIONAL DE LOS DERECHOS HUMANOS Y SU RELACIÓN CON LAS NUEVAS TECNOLOGÍAS

La preocupación de los Estados por los derechos de las personas tuvo como catalizador las consecuencias de la Segunda Guerra Mundial (1939-1945), que ocasionaron la muerte de entre 35 a 70 millones de personas. Entre las víctimas, se encontraban judíos, romaníes, eslavos, personas con discapacidad y personas homosexuales, grupos que fueron brutalmente asesinados por las autoridades de la Alemania nazi debido a su presunta «inferioridad racial y biológica» (Royde-Smith, s/f).

A raíz de ello, la comunidad internacional empezó a tomar conciencia de la importancia de hacer valer los derechos de los individuos en el orden internacional, creándose la Carta de la ONU (1945), la cual fijó estándares de carácter universal sobre el alcance de los derechos humanos (Salmón, 2019, p. 146). Así, entre sus propósitos, el artículo 1.3 de la Carta señala que los Estados parte deben «[r]ealizar la cooperación internacional en [...] el desarrollo y estímulo del respeto a los derechos humanos y a las libertades fundamentales de todos, sin hacer distinción por motivos de raza, sexo, idioma o religión».

Con dicho contexto, los primeros pasos para regular los derechos humanos en el ámbito internacional se emprendieron en 1948 con la DADDH y la DUDH, adoptadas respectivamente en mayo y diciembre de ese año. Ambas declaraciones reconocen que los seres humanos nacen iguales en dignidad y enlistan una serie de derechos que les corresponden a todos sin distinción. Desde aquel momento histórico, «los Estados han suscrito una diversidad de tratados que consagran derechos humanos a favor de las personas que se encuentran bajo su jurisdicción» (Salmón, 2019, p. 147).

En el ámbito del SUDH, en 1966, la Asamblea General de la ONU adoptó dos tratados que moldearon aún más a los derechos humanos: el PIDCP y el PIDESC. Dichos tratados, junto a los dos Protocolos Facultativos del PIDCP y la DUDH, se conocen como la Carta Internacional de Derechos Humanos (ONU, s/f b). Cabe destacar que, pocos años más tarde, en el marco del SIDH, se adoptó la CADH (1969), la cual fue complementada en 1988 con la adopción del Protocolo de San Salvador.

El cuerpo normativo del DIDH ha ido ampliándose a lo largo del tiempo debido a diversos factores. De manera progresiva se han sumado nuevos tratados que reconocen las necesidades particulares de determinados grupos humanos y, en respuesta, regulan a su favor derechos específicos. Por ejemplo, se han adoptado tratados para proteger a grupos que enfrentan entornos que injustamente les restringen o impiden desarrollar uno o varios aspectos de sus vidas, quedando sujetos a una situación de vulnerabilidad y, por ende, a un mayor riesgo de afectación a sus derechos (Lara, 2015, p. 26). Este es el caso de las mujeres, los/as NNA, las personas con discapacidad o las personas de edad, que constituyen grupos históricamente discriminados cuya especial situación de vulnerabilidad ha propiciado la adopción de tratados internacionales orientados a lograr que ejerzan sus derechos y libertades de manera efectiva.

En paralelo, en las últimas décadas, se han intensificado diversas problemáticas de alcance global cuyo impacto en las condiciones de vida de las personas y en la satisfacción de sus derechos ha exigido que se adopten medidas principalmente por parte de los Estados, y, en segundo plano, por parte de las organizaciones internacionales. Entre estas circunstancias se ubican las consecuencias ya visibles del cambio climático; las causas y los efectos de los conflictos armados que resultan en desplazamientos forzosos; la agudización de la migración sin

una debida respuesta multiactor; el agravamiento de las crisis humanitarias y económicas; entre otros.

A estos escenarios se suma de manera más reciente la preocupación sobre los desafíos que trae consigo el acelerado desarrollo de las tecnologías para la protección de los derechos humanos y que aboga por la concreción de un nuevo régimen internacional en la materia (Orias, 2022, p. 214). En cierta medida, las tecnologías han sido materia de regulación internacional dada su importancia para el proyecto de vida de las personas y los propios Estados.⁴ No obstante, a nivel mundial, existe una discusión vigente respecto a si la nueva realidad que se presenta ante la comunidad internacional amerita la «creación» de nuevos derechos humanos específicos para a) reducir las brechas digitales;⁵ y b) proteger, desde un enfoque interseccional, a la población frente a las amenazas que traen consigo las nuevas tecnologías.

En relación con lo primero, aunque el uso generalizado de las TIC, particularmente del Internet, se ha extendido a numerosas esferas, lo cierto es que a nivel internacional se ha reconocido que «la falta de acceso a tecnologías y servicios asequibles y confiables sigue siendo un problema fundamental en muchos países en desarrollo», lo que revela la imperiosa necesidad de desplegar «todos los esfuerzos posibles para reducir el precio de las tecnologías de la información y las comunicaciones y del acceso a la banda ancha» (Asamblea General de las Naciones Unidas, 2018, párr. 25). A lo anterior deben sumarse, de manera central pero no exclusiva, las brechas basadas en variables sociodemográficas, tales como género, nivel de urbanización, nivel de renta, nivel educativo y edad.

Frente a la situación descrita, el ACNUDH ha señalado que «[l]os Estados y las empresas deben velar por que el desarrollo y despliegue de las TIC, incluidas las nuevas tecnologías basadas en datos, estén guiados y regulados por el derecho internacional de los derechos humanos, incluidos los principios de la igualdad de género [...]» (2017, párr. 46). Esto ha derivado en que el debate en torno a la necesidad de establecer regulaciones para las grandes empresas tecnológicas se acentúe de manera progresiva. Este debate ha sido incluso impulsado por distintas comunidades alrededor del mundo, como la rohinyá en Myanmar, que exigen justicia y rendición de cuentas debido a los daños a los derechos humanos que el modelo empresarial de las grandes empresas tecnológicas ha causado o contribuido a causar.⁶ A pesar de que actualmente no existe un tratado vinculante en la materia,⁷ existen instrumentos de *soft law* como los Principios Rectores de las Naciones Unidas sobre Empresas y Derechos Humanos⁸ y las Líneas Directrices para Empresas Multinacionales sobre Conducta Empresarial Responsable⁹

⁴ Por ejemplo, en la Carta de la OEA, se señala que los Estados miembros se comprometen a aunar esfuerzos para que sus pueblos alcancen un desarrollo integral, lo cual abarca el campo tecnológico (artículo 30). Asimismo, en el Protocolo de San Salvador, se consagra el derecho de toda persona a «gozar de los beneficios del progreso científico y tecnológico» (artículo 14).

⁵ Al respecto, se han identificado tres principales niveles de brecha digital: acceso, uso y apropiación de TIC por individuos y organizaciones (públicas o privadas), que retrasan el aprovechamiento de estas tecnologías (Gómez, Alvarado, Martínez y Díaz de León, 2018, p. 52).

⁶ Para mayor información, revítese el siguiente informe de Amnistía Internacional: <https://www.amnesty.org/es/latest/news/2022/09/myanmar-facebooks-systems-promoted-violence-against-rohingya-meta-owes-reparations-new-report/>.

⁷ Pese a ello, cabe destacar que las Naciones Unidas tiene la intención de emitir un instrumento legalmente vinculante que regule las actividades de las empresas transnacionales. Este lo está desarrollando el Grupo de Trabajo intergubernamental de composición abierta sobre las empresas transnacionales y otras empresas en relación con los derechos humanos, creado en el 2014 a raíz de la Resolución 26/9.

⁸ Entre los principios recogidos, destacan los principios fundacionales: «1) Los Estados deben proteger contra las violaciones de los derechos humanos cometidas en su territorio y/o su jurisdicción por terceros, incluidas las empresas. A tal efecto deben adoptar las medidas apropiadas para prevenir, investigar, castigar y reparar esos abusos mediante políticas adecuadas, actividades de reglamentación y sometimiento a la justicia; y 2) Los Estados deben enunciar claramente que se espera de todas las empresas domiciliadas en su territorio y/o jurisdicción que respeten los derechos humanos en todas sus actividades».

⁹ En la Enmienda de 2023, se señala que «En el contexto del desarrollo, la financiación, la venta, la concesión de licencias, el comercio y el uso de tecnología, incluida la recopilación y el uso de datos, así como la investigación

de la OCDE, que buscan prevenir y abordar los impactos a los derechos humanos vinculados al desarrollo y uso de las nuevas tecnologías por parte de empresas, Gobiernos, organizaciones no gubernamentales y otros actores, incluidos los usuarios.

Respecto al impacto diferenciado de las nuevas tecnologías, la CIDH y su RELE han llamado a los Estados a adoptar medidas para reducir las brechas digitales, resaltando que el Internet constituye hoy una herramienta crucial para potenciar la calidad de vida de las personas, «así como para la realización de los derechos fundamentales como el acceso a la información, los derechos de reunión y asociación, los derechos políticos, el derecho a la educación, el derecho a participar en la vida cultural, el derecho a la salud, entre otros» (CIDH, 2021a).

En este contexto, ¿se debe reconocer el acceso a Internet como un derecho humano? Si bien existen diversos argumentos a favor y en contra de dicho reconocimiento, es innegable que, en la actualidad, no tener acceso a Internet limita el ejercicio de diversos derechos. Así, si consideramos que «progresivamente un mayor número de servicios, incluso vinculados con derechos de ciudadanía, se están ofreciendo exclusivamente vía online, el impacto que tienen estas formas de exclusión es aún mayor» (Sáinz, Arroyo y Castaño, 2020, p. 32).

Ciertamente, el debate sobre la creación de nuevos derechos digitales surge como respuesta a los desafíos y las amenazas planteados por las nuevas tecnologías. A pesar de los notables beneficios que estas tecnologías han aportado, también han generado preocupaciones, principalmente, en relación con la privacidad y la libertad de información. Cuestiones como la recopilación masiva de datos personales, la vigilancia en línea y la manipulación de la información se han convertido en preocupaciones cada vez más apremiantes. La falta de una regulación adecuada y de salvaguardias destinadas a proteger la privacidad de las personas puede llevar a la exposición no deseada de información personal. Además, la propagación de la desinformación en línea plantea la amenaza de socavar la libertad de información y distorsionar la percepción de la realidad.

Aunque las mencionadas amenazas han sido objeto de atención a nivel internacional, en los últimos años han surgido nuevos desafíos que todavía no se encuentran debidamente abordados por los distintos actores de la comunidad internacional y, como parte de esta, por los Estados en la gestión de sus asuntos internos. Por ejemplo, cobra fuerza de manera progresiva la discusión en torno a las posibilidades y los retos que traen consigo las neurotecnologías¹⁰ y, de modo más aterrizado, si es que los avances de esta manifestación de la tecnología deberían estar acompañados de la construcción de un nuevo marco jurídico internacional de derechos humanos destinados específicamente a proteger el cerebro y su actividad (Orias, 2022, p. 216).

Resulta interesante, además, destacar que este debate ha sido impulsado por la propia comunidad científica. De hecho, fue el neurobiólogo Rafael Yuste quien, en el 2017, sustentó la necesidad de reconocer cuatro neuroderechos.¹¹ Si bien, al igual que para el resto de tecnologías,

científica y la innovación, las empresas deberían observar las Líneas Directrices y cumplir con la legislación y los requisitos nacionales aplicables, incluidos los relativos a la privacidad y protección de datos y a las regulaciones de control de exportaciones» (p. 51).

¹⁰ Frente a la aparición de las neurotecnologías, el Comité Jurídico Interamericano aprobó la Declaración sobre Neurociencia, Neurotecnologías y Derechos Humanos: Nuevos Desafíos Jurídicos para las Américas, la cual contempla las siguientes inquietudes: 1) Condicionamiento de la personalidad y pérdida de memoria; 2) Intervenciones legítimas en materia de salud, integridad física y mental; 3) Privacidad mental y protección de datos neuronales obtenidos a partir del uso de neurotecnologías; 4) Igualdad de acceso y no discriminación en el uso de las neurotecnologías; y 5) Libertad de expresión y acceso a la información pública.

¹¹ Estos son los siguientes: «i) El Derecho a la identidad personal y derecho al libre albedrío, que buscan que la identidad de las personas no se diluya o se vea influenciada por los algoritmos en la toma de decisiones; ii) el Derecho a la privacidad y consentimiento, mediante el cual se protege la inviolabilidad de los neuro datos que generan los cerebros humanos; iii) el Derecho al acceso equitativo a las tecnologías, al garantizar su acceso y beneficios para todos

aún no existen disposiciones internacionales vinculantes en materia de neurotecnologías, en el 2021, la OEA aprobó la Declaración sobre Neurociencia, Neurotecnologías y Derechos Humanos: Nuevos Desafíos Jurídicos para las Américas; y, la UNESCO, la *Recomendación sobre la Ética de la Inteligencia Artificial*. Ambos instrumentos hacen hincapié en que las neurotecnologías deben preservar la dignidad y autonomía humanas.

En vista de lo anterior, se puede afirmar que existen algunos instrumentos internacionales que contemplan el impacto de las tecnologías en los derechos humanos y que establecen ciertos parámetros de protección y garantías mínimas que los Estados deben cumplir a fin de proteger a su población y acortar las brechas digitales. La evolución de las tecnologías y los nuevos retos que se han ido presentando en los últimos años a raíz de su proliferación y uso inadecuado revelan la importancia de plantear respuestas adecuadas y oportunas no solo a nivel estatal, sino de manera coordinada con organizaciones internacionales. Tal es la relevancia de la materia que, por ejemplo, el Secretario General de la ONU, António Guterres, declaró que «la inteligencia artificial debe beneficiar a todos, incluida la tercera parte de la humanidad que aún está desconectada del Internet», e insistió en la necesidad de llegar urgentemente a un consenso sobre cuáles deben ser las normas que guíen su uso (Noticias ONU, 2023).

Los retos planteados hasta este punto a manera de ejemplo y con el objetivo de estimular la reflexión sobre el tópico de este informe se abordarán en profundidad en los siguientes apartados a partir de un análisis delineado por el enfoque de derechos humanos.

4. ¿PUEDEN LAS NUEVAS TECNOLOGÍAS SOCAVAR LOS DERECHOS HUMANOS? ANÁLISIS SOBRE ESCENARIOS DE POSIBLES AMENAZAS

El desarrollo de las nuevas tecnologías y su uso en la vida de las personas avanza sin precedentes en comparación con años anteriores. Sin embargo, dichos avances tecnológicos no van de la mano con la creación y el desarrollo de los mecanismos de regulación que se necesitan, por lo que resulta preocupante advertir la falta de respuestas por parte de los Estados y las organizaciones ante los nuevos desafíos y amenazas que dichas tecnologías causan o pueden causar a la vida de las personas y, por ende, a sus derechos humanos.

En función de lo anterior, esta sección del informe pretende abordar las amenazas que generan las nuevas tecnologías; por un lado, en los derechos de privacidad, libertad de expresión y participación política; y, por otro lado, en los derechos a la salud, a la educación y al trabajo. Para ello, se desarrolla el marco normativo de cada derecho mencionado a la luz del DIDH, su contenido material y las obligaciones de los Estados respecto a cada uno. Seguidamente, se examinan los avances y las tareas pendientes que surgen a raíz de la relación entre las nuevas tecnologías y los derechos bajo estudio.

y todas, y iv) el Derecho a la protección contra sesgos y discriminación, que prevé evitar las brechas y desigualdades como efecto de la aplicación de las neurotecnologías (Orias, 2022, p. 216). Las negritas son nuestras.

4.1. AMENAZAS A LOS DERECHOS A LA PRIVACIDAD, LIBERTAD DE EXPRESIÓN Y PARTICIPACIÓN POLÍTICA

4.1.1. Derecho a la privacidad

En el marco del SUDH, el derecho a la privacidad está consagrado en el artículo 12¹² de la DUDH y el artículo 17¹³ del PIDCP. El SIDH contempla también este derecho a partir de lo dispuesto en el artículo V¹⁴ de la DADDH y el artículo 11¹⁵ de la CADH. Dichos instrumentos coinciden al señalar que el derecho a la privacidad implica que ninguna persona puede ser objeto de injerencias arbitrarias en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación. Asimismo, en virtud de este derecho, toda persona debe contar con la protección de la ley frente a dichas injerencias.

En el caso *Artavia Murillo contra Costa Rica*, la Corte IDH ha señalado que la vida privada incluye «la forma en que el individuo se ve a sí mismo y cómo decide proyectarse hacia los demás y es una condición indispensable para el libre desarrollo de la personalidad» (2012, párr. 143). En atención a lo anterior, podemos señalar que este derecho contiene dos aspectos: a) la libertad de aislarnos de las demás personas en términos generales; y b) el derecho de controlar la información que se produce de nosotros mismos y de nuestras familias (García, s/f, p. 191). Mientras que el primero se refiere a un ámbito personalísimo en tanto implica protegernos del resto; el segundo se refiere a un ámbito público en tanto podemos decidir cómo proyectarnos mediante nuestra información —que es o puede ser— compartida con terceros.

Respecto a las obligaciones que tienen los Estados en relación con este derecho, según el Comité de Derechos Humanos (1998), en referencia al derecho a la intimidad, ha indicado en su Observación General n.º 16 que aquellos deben adoptar medidas legislativas y de otra índole para evitar que se produzcan injerencias ilegales y arbitrarias generadas por el propio Estado o particulares (párr. 1). Sin perjuicio de ello, el Comité también señala que, en tanto ningún derecho puede ejercerse de forma absoluta, el derecho a la privacidad puede ser sujeto de injerencias autorizadas, las cuales deben estar señaladas en las leyes y los reglamentos (1998, párr. 3). Como puede ser el caso de un allanamiento al domicilio autorizado por un juez, o el levantamiento del secreto bancario en el marco de una investigación penal.

Ahora bien, la obligación de proteger el derecho a la privacidad por parte de los Estados abarca los dos aspectos desarrollados y su ejercicio en los espacios físicos, pero también en los digitales. Pensemos, por ejemplo, en toda la información almacenada de nuestras conversaciones a través de las *apps* o en las grabaciones almacenadas en la nube mediante nuestras interacciones con equipos de IA como Alexa.¹⁶ ¿Será posible controlar nuestros datos almacenados? ¿Es posible saber quiénes tienen acceso a ellos y para qué?

¹² «Artículo 12.-

Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques».

¹³ «Artículo 17.-

1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación.

2. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques».

¹⁴ «Artículo V. Toda persona tiene derecho a la protección de la Ley contra los ataques abusivos a su honra, a su reputación y a su vida privada y familiar».

¹⁵ «Artículo 11. Protección de la Honra y de la Dignidad

1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad.

2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.

3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques».

¹⁶ Para mayor información, véase la respuesta de Amazon a la pregunta 2 de las sección «Preguntas frecuentes» sobre

Al respecto, el Comité es claro en señalar que la vigilancia de las correspondencias, ya sea por medios electrónicos o de otra índole, así como la intervención y grabación de conversaciones y comunicaciones telefónicas o de otro tipo deben prohibirse. Agrega que la recopilación y el registro de información personal en computadoras, bancos de datos y otro tipo de dispositivos deben estar reglamentados por ley, y que toda persona debe verificar si hay datos suyos almacenados en archivos automáticos de datos, saber cuáles son y con qué fin se encuentran ahí, así como conocer quién tiene acceso a dichos archivos y, de ser el caso, pedir su rectificación o eliminación (1998, párr. 10). En ese orden de ideas, la Asamblea General de las Naciones Unidas (2015) exhortó a los Estados a «proporcionar acceso a un recurso efectivo a las personas cuyo derecho a la privacidad haya sido violado mediante la vigilancia ilícita o arbitraria, de conformidad con las obligaciones internacionales en materia de derechos humanos» (párr. 4).

Por su parte, el ACNUDH (2018) ha indicado que tecnologías como el Big Data y la IA (véase *supra* apartado 2) se vuelven más poderosas y amenazan con crear un entorno digital intrusivo, en tanto los Gobiernos y las empresas pueden realizar labores de vigilancia, análisis, predicción e incluso pueden llegar a manipular el comportamiento humano en una medida nunca antes vista, lo que plantea serios desafíos y riesgos a la dignidad humana y los derechos humanos si no se abordan con el cuidado que se requiere (párr. 1). En esa línea, identifica dos grupos de amenazas: el uso creciente de datos personales por parte de los Estados y sujetos privados; y la vigilancia e interceptación de las comunicaciones por parte de los Estados.

En la primera amenaza señalada se incluye: a) el aumento de la huella digital que reúne y utiliza grandes cantidades de información y que en su mayoría no cuenta con el consentimiento de los titulares; b) el intercambio y la fusión de datos por parte de las empresas y los Estados, lo que coloca en indefensión a las personas al no poder controlar el manejo de su información personal y el cómo pueda utilizarse; c) la recopilación de datos biométricos como huellas dactilares, ADN, reconocimiento facial que pueden utilizarse para fines contrarios, como seguimiento ilegal o robo de identidad; y d) el aumento de la capacidad de análisis basadas en macrodatos e IA.

Con relación a la segunda amenaza se tiene: a) la vigilancia a gran escala realizada por los Estados bajo la excusa de velar por la seguridad nacional; b) el acceso directo por parte de los Estados a los datos de los usuarios de las empresas, sin contar con las garantías procesales que se requieren para ello; c) la piratería informática que pueden usar los Gobiernos para interceptar los dispositivos de las personas; d) los intentos de los Estados y agentes privados por debilitar el cifrado y el anonimato para acceder a la información privada de las personas; e) el intercambio de información de inteligencia entre Gobiernos sin un marco legal establecido y formas de supervisión; y f) el acceso transfronterizo a los datos de las empresas en el extranjero.

Un ejemplo de lo anterior es el caso del Estado colombiano que realizó contrataciones desde el 2013 con empresas de tecnología para fortalecer su sistema de vigilancia, la Plataforma Única de Monitoreo y Análisis, mediante el uso de *exploits*, un *software* malicioso hecho a la medida de la persona a la que se le van a interceptar sus equipos, sin que la persona pueda advertirlo. Al respecto, el Gobierno señaló que dicha tecnología solo se usaba en el marco de investigaciones judiciales; sin embargo, no se tenía información transparente sobre los verdaderos alcances del uso de esta tecnología que podía invadir la privacidad de las personas, sin que estas tuvieran conocimiento de los *hackeos* (Sáenz y Botero, 2015).

Alexa y los dispositivos Alexa:

<https://www.amazon.com/-/es/gp/help/customer/display.html?nodeId=201602230>.

Otro ejemplo es el caso *Big Brother Watch v. UK*¹⁷ (2021), que fue resuelto por el TEDH, el cual declaró la violación del derecho a la privacidad y protección de datos consagrado en el artículo 8¹⁸ del CEDH. Si bien el TEDH señaló que la vigilancia estatal a gran escala puede estar permitida, en el caso en concreto algunas prácticas eran arbitrarias en tanto no existían salvaguardias adecuadas para proteger a las personas contra la vigilancia masiva y la recopilación indiscriminada de datos. Asimismo, había un acceso indiscriminado de datos de forma amplia y discrecional sin ninguna justificación. Tampoco existió una supervisión independiente de dichas prácticas y, por último, la legislación no era lo suficientemente clara sobre su naturaleza y alcance, lo que dificultó que las personas pudieran comprender y prever las implicaciones para su privacidad.

Con relación a la recopilación de grandes datos a manos de empresas privadas, resulta relevante mencionar el caso de Alemania, que prohibió el uso de los «robots amigos» de niños. En particular, la Agencia Federal de Redes de Alemania prohibió el uso de este juguete debido a que el micrófono y la conexión de Bluetooth integrados lo convierten en un posible instrumento de espionaje no permitido por la ley (El Mundo, 2017). En el caso en cuestión, el Estado comprendió que con estos juguetes creados con IA se corre el riesgo de que se utilicen como instrumentos de espionaje o que puedan ser *hackeados* por extraños. Además, se sabe que hay una gran cantidad de datos e información que dichos juguetes almacenan y que están en manos de las empresas creadoras, las cuales pueden utilizar dicha información para crear nuevos perfiles de juguetes que se ajusten a las necesidades de sus usuarios (Hutt, 2018). Sin embargo, cabe plantearse las siguientes preguntas: ¿hasta dónde son responsables las empresas de los datos almacenados de los niños?, ¿debe haber lineamientos en la creación de algoritmos para este tipo de juguetes?, ¿cuáles serían?

Los casos planteados ponen en contexto las amenazas e injerencias arbitrarias a las que la privacidad está expuesta: desde que las comunicaciones personales sean intervenidas por el Estado sin que esto sea ampliamente conocido hasta la vigilancia regulada por ley por parte de los Estados, pero que no cumple con los parámetros establecidos por el DIDH, sea por la falta de claridad y precisión, o por no contar con mecanismos de protección o alguna institución que supervise dichas decisiones.

Finalmente, en lo relativo a los avances en la región de América Latina, Derechos Digitales (2020a) destacó la actualización de la normativa sobre protección de datos, así como la regulación sobre interceptación de comunicaciones, grabaciones e interceptación de sistemas informáticos desde la justicia penal (p. 4). Al margen de dichos avances, la referida organización destacó que aún persiste la necesidad de regular los ecosistemas digitales, definidos como «el conjunto de infraestructuras y prestaciones asociadas a la provisión de contenidos y servicios a través de internet» (Katz, 2015). La proliferación de dichos ecosistemas viene aparejada con la problemática de la extraterritorialidad, «donde debido a la naturaleza de los servicios que se prestan a través de internet, estos no se ven enmarcados en un Estado concreto por lo que la legislación a nivel nacional no podría ser aplicable» (Pérez y Núñez, 2017, p. 1281). Para remediar ello, será necesario que los Estados uniformicen su normativa en la materia, a fin de garantizar la aplicación de un mismo marco legal independientemente del país de origen y

¹⁷ La demanda fue presentada ante el TEDH en el 2013; en esta se argumentó que las prácticas de vigilancia masiva de Reino Unido, en particular la recopilación de datos de comunicaciones electrónicas, violaban el derecho a la privacidad y protección de datos, conforme al CEDH.

¹⁸ «Artículo 8. Derecho al respeto a la vida privada y familiar

1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.

2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás».

así resguardar los derechos de los usuarios (Pérez y Núñez, 2017, p. 1281). Finalmente, en relación con los datos biométricos, Derechos Digitales hizo hincapié en que hay una tendencia en la región sobre la regulación del uso de huellas dactilares y, en menor medida, de pruebas de ADN; pero, en la práctica, también se usa el escaneo facial y ocular, sin que se cuente con regulación al respecto (Derechos Digitales, 2020a, pp. 28-29).

4.1.2. Libertad de expresión

El derecho a la libertad de expresión está reconocido en el artículo 19 de la DUDH¹⁹ y el artículo 19²⁰ del PIDCP, así como en el artículo IV²¹ de la DADDH y el artículo 13²² de la CADH. Este derecho comprende la facultad de toda persona para buscar, recibir y difundir información de todo tipo y en diversos medios, incluidos los digitales. Conforme a lo señalado por la Corte IDH (1985) en su Opinión Consultiva n.º 5, la libertad de expresión tiene dos componentes: uno individual, que permite a las personas difundir sus opiniones e información a través de diversos medios; y otro colectivo, que implica el derecho de la sociedad en su conjunto a conocer opiniones y noticias de terceros (párrs. 31 y 32), conocido también como el derecho de acceso a la información.

A través de su jurisprudencia, la Corte IDH ha contribuido de forma significativa en el desarrollo del derecho a la libertad de expresión en la región de América y el Caribe, destacando que, aunque este derecho es esencial en una sociedad democrática, no es absoluto, y pueden existir restricciones que sean legales, necesarias y proporcionales a fines legítimos en una sociedad democrática, según se estableció en la sentencia del caso Herrera Ulloa vs. Costa Rica (2004, párr. 120).

¹⁹ «Artículo 19.-

Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión».

²⁰ «Artículo 19.-

1. Nadie podrá ser molestado a causa de sus opiniones.

2. Toda persona tiene derecho a la libertad de expresión; este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección.

3. El ejercicio del derecho previsto en el párrafo 2 de este artículo entraña deberes y responsabilidades especiales. Por consiguiente, puede estar sujeto a ciertas restricciones, que deberán, sin embargo, estar expresamente fijadas por la ley y ser necesarias para: a) Asegurar el respeto a los derechos o a la reputación de los demás; b) La protección de la seguridad nacional, el orden público o la salud o la moral públicas».

²¹ «Artículo IV. Toda persona tiene derecho a la libertad de investigación, de opinión y de expresión y difusión del pensamiento por cualquier medio».

²² «Artículo 13. Libertad de Pensamiento y de Expresión

1. Toda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección.

2. El ejercicio del derecho previsto en el inciso precedente no puede estar sujeto a previa censura sino a responsabilidades ulteriores, las que deben estar expresamente fijadas por la ley y ser necesarias para asegurar:

a) el respeto a los derechos o a la reputación de los demás, o

b) la protección de la seguridad nacional, el orden público o la salud o la moral públicas.

3. No se puede restringir el derecho de expresión por vías o medios indirectos, tales como el abuso de controles oficiales o particulares de papel para periódicos, de frecuencias radioeléctricas, o de enseres y aparatos usados en la difusión de información o por cualesquiera otros medios encaminados a impedir la comunicación y la circulación de ideas y opiniones.

4. Los espectáculos públicos pueden ser sometidos por la ley a censura previa con el exclusivo objeto de regular el acceso a ellos para la protección moral de la infancia y la adolescencia, sin perjuicio de lo establecido en el inciso 2.

5. Estará prohibida por la ley toda propaganda en favor de la guerra y toda apología del odio nacional, racial o religioso que constituyan incitaciones a la violencia o cualquier otra acción ilegal similar contra cualquier persona o grupo de personas, por ningún motivo, inclusive los de raza, color, religión, idioma u origen nacional».

Por su parte, el Comité de Derechos Humanos (2011) ha indicado que el derecho a la libertad de expresión abarca la búsqueda, recepción y difusión de información e ideas sin restricciones geográficas. Este derecho incluye la comunicación de diversas opiniones y pensamientos, como el político, cultural, periodístico, religioso y publicidad comercial. Además, protege todas las formas de expresión que incluyen palabras escritas y habladas, lenguaje de signos, imágenes y objetos artísticos, y se extiende a una amplia variedad de medios, desde libros y periódicos hasta medios electrónicos e Internet (párrs. 11 y 12). Aunque este derecho también cubre expresiones que pueden considerarse ofensivas, su limitación está sujeta a ciertas restricciones como lo hemos señalado en el párrafo anterior, y bajo ninguna circunstancia amparará a los mensajes de propaganda en favor de la guerra ni a los discursos de odio nacional, racial o religioso.

En relación con las obligaciones de los Estados en esta materia, la CIDH a través de su Relatoría Especial para la Libertad de Expresión publicó el informe *Libertad de expresión en internet* (2013). En dicho informe se establecen cuatro principios rectores de la libertad de expresión en Internet: a) acceso universal; b) pluralismo; c) no discriminación; y d) privacidad.

Sobre el primer principio, los Estados deben garantizar que todas las personas tengan acceso a Internet, lo que incluye expandir la infraestructura y adoptar medidas para que especialmente las personas o los grupos tradicionalmente marginados puedan acceder. El segundo está orientado a que los Estados promuevan el pluralismo informativo, así como a maximizar el número y la diversidad de voces e ideas. En virtud del tercer principio, los Estados deben tomar las medidas necesarias para asegurar que todas las personas, especialmente las que se encuentran en situación de vulnerabilidad, puedan difundir contenidos u opiniones en términos de igualdad. El fin último de este principio es la neutralidad de la red. El cuarto principio se enfoca en la privacidad como elemento esencial del ejercicio de la libertad de expresión (2013, párrs. 15-24).

En su conjunto, estos principios cobran especial relevancia en tanto Internet tiene un potencial sin precedentes de empoderar a las personas, en general donde sea que se encuentren, al permitirles buscar, recibir y difundir ideas e información, a diferencia de otros medios de comunicación que suelen ser unidireccionales, como la radio o televisión. Sin embargo, como bien lo reconoce la UNESCO (2021b), la IA y las TIC avanzadas pueden promover la libertad de expresión, pero, al mismo tiempo, plantean desafíos y cuestiones relacionadas con la libertad de expresión (p. 39).

En esa línea, Orenca (2022) ha identificado algunas amenazas a esta libertad derivadas del uso de la IA y los algoritmos, como, por ejemplo, el perfilado y la presentación de contenidos sobre la base de nuestras elecciones y navegación en Internet, pero promovidas por la IA; lo que provoca que nuestra libertad para acceder o buscar información sea relativa al «esconder» información que no encaja en el perfil creado a partir de los datos que previamente se han recopilado (pp. 24-25). Ello se debe a que la IA influye en la manera en que las personas podemos acceder a la información en línea mediante el uso de los motores de búsqueda que utilizan algoritmos de aprendizaje automático con la finalidad de adaptar el contenido que se presenta al usuario (UNESCO, 2021a, p. 40).

Si bien inicialmente puede parecer positivo que el usuario acceda a información según sus preferencias o necesidades previamente mostradas, también es cierto que esto limita su libertad de expresión, en tanto no podrá acceder fácilmente a información variada y hasta contradictoria a sus propias ideas. Landa señala que el diseño y funcionamiento de los algoritmos puede llevar a la fragmentación informativa y favorecer a determinadas plataformas o conglomerado de medios de comunicación en el caso de que el algoritmo presente algún

sesgo (2023, pp. 77-78). Lo anterior constituye una seria amenaza relacionada con el principio de pluralismo informativo señalado anteriormente.

Por otro lado, también constituye una amenaza la moderación del contenido a través del bloqueo y la eliminación de información que en muchos casos utilizan algoritmos de Machine Learning (véase la Tabla 1). Dicha moderación es problemática, ya que se determina a partir de sesgos y criterios subjetivos que no responden a los criterios de restricción de derechos del DIDH: legalidad, necesidad y proporcionalidad. Agrega Orenga que el algoritmo no está diseñado o preparado para reconocer la ironía, la burla o el sarcasmo, por lo que el bloqueo o la eliminación de contenido bajo este contexto constituye una censura a la libertad de expresión (2022, p. 27).

Algunos casos que dan cuenta de los retos hasta aquí reseñados son los vinculados con la libertad de expresión en contextos de protestas. Al respecto, la CIDH (2022a) expresó su preocupación por el «ciberpatrullaje» para combatir el «terrorismo digital» que realizó el Estado colombiano con la finalidad de ubicar noticias falsas especialmente relacionadas con el actuar de las fuerzas públicas durante las protestas en el 2021 mediante el bloqueo y la eliminación de URL y páginas webs que tenían material relacionado con las protestas (párrs. 264-266). Situación similar es la de Cuba, en donde se utilizan categorías genéricas como «moralidad pública», «subversión social» e «indisciplina social» en leyes de ciberseguridad para limitar de forma abusiva derechos a la libertad de expresión y a la protesta (párr. 330).

En la audiencia temática Inteligencia Digital, Ciberseguridad y Libertad de Expresión, desarrollada por la CIDH en el 2018, se compartió información sobre las limitaciones a la libertad de expresión por parte de los Estados en el marco de la implementación del Convenio de Budapest sobre Ciberdelincuencia,²³ ya que los Estados de la región están generando legislación orientada a regular los discursos de odio mediante el bloqueo de contenidos digitales, que afecta principalmente a colectivos en situación de vulnerabilidad (Instituto Panamericano de Derecho y Tecnología, 2018).

En relación con la vigilancia masiva y selectiva, la CIDH y la RELE (CIDH, 2023a) han documentado en los últimos años varios casos de espionaje en México a través del *software* Pegasus,²⁴ como el presunto espionaje a miembros del Centro de Derechos Humanos Miguel Agustín Pro Juárez, posiblemente por su labor de defensa de los derechos humanos. También se ha informado del uso de este *software* para vigilar a autoridades de alto nivel y a una variedad de personas, incluyendo periodistas, defensores de derechos humanos e inclusive un juez de la Corte IDH. Asimismo, la CIDH, la RELE y la OACNUDH han documentado que, en El Salvador, al menos 35 personas de medios de comunicación y organizaciones de la sociedad civil salvadoreña fueron intervenidas en sus teléfonos por el mismo *software*, siendo la mayoría integrantes de medios periodísticos de investigación como *El Faro* (CIDH, 2022b).

²³ El Convenio de Budapest fue abierto a la firma de Estados miembros y no miembros del Consejo de Europa en el 2001. Es el primer tratado internacional sobre delitos cometidos a través de Internet, especialmente los vinculados a derechos de autor, fraude informático, pornografía infantil y violaciones de las redes. Su principal objetivo, según el preámbulo del tratado, es aplicar una política criminal común para enfrentar el ciberdelito, especialmente mediante legislación adecuada y cooperación internacional. Argentina, Brasil, Canadá, Chile, Colombia, Costa Rica, República Dominicana, Panamá, Paraguay, Perú y Estados Unidos se han adherido al tratado en mención.

²⁴ Pegasus es un sofisticado *software* creado por la empresa israelí NSO Group. Este funciona mediante el perfeccionamiento de la técnica del *spear-phishing*; es decir, envía mensajes o llamadas al dispositivo que se quiere infectar. Una vez instalado en el teléfono, este *software* es capaz de acceder a la información del propietario y a varias funciones del teléfono (activar el micrófono, la cámara, geolocalizar, etc). Según la empresa creadora, el objetivo de este *software* es combatir el terrorismo y la delincuencia. Sin embargo, se han presentado varios casos de espionaje a figuras políticas en Latinoamérica.

La CIDH ha sido contundente al indicar que las prácticas de vigilancia o espionaje no solo vulneran el derecho a la privacidad, como se ha señalado en el acápite anterior, sino que también pueden poner en riesgo la integridad de periodistas y defensores de derechos humanos. Adicionalmente a ello, se debe resaltar que este tipo de prácticas promueve la intimidación y autocensura por miedo a represalias y persecuciones, especialmente cuando se trata de expresar ideas u opiniones críticas. Por ello, no solo se ve afectada la libertad de expresión en su dimensión individual, sino también en su dimensión colectiva en tanto la población tampoco podrá acceder a información crítica y diversa.

En vista de lo anterior, se puede concluir que la falta de transparencia y rendición de cuentas en el uso de IA y nuevas tecnologías representa un desafío crítico para la garantía del derecho a la libertad de expresión. Por lo que es imperativo que estas tecnologías sean desarrolladas y operadas de acuerdo con los estándares y las obligaciones del DIDH para abordar las amenazas que plantean y salvaguardar este derecho fundamental en la era digital.

4.1.3. Derecho a la participación política

En el marco del SUDH, el derecho a la participación política está reconocido en el artículo 21²⁵ de la DUDH y el artículo 25²⁶ del PIDCP. A nivel del SIDH, este derecho encuentra su reconocimiento en el artículo XX²⁷ de la DADDH y el artículo 23²⁸ de la CADH, que comprende el derecho de participar en los asuntos públicos, de forma directa a través de las candidaturas para acceder a cargos políticos de elección popular, o de forma indirecta eligiendo a las autoridades y representantes.

Asimismo, incluye el derecho a votar y ser elegido en elecciones universales mediante voto secreto, así como a tener acceso a las funciones públicas del país en condiciones de igualdad. Estas distintas facetas de la participación requieren contar con información para elaborar una propuesta electoral (planes de gobierno, oferta electoral), y, luego, una vez elegidas las

²⁵ «Artículo 21.-

1. Toda persona tiene derecho a participar en el gobierno de su país, directamente o por medio de representantes libremente escogidos.
2. Toda persona tiene el derecho de acceso, en condiciones de igualdad, a las funciones públicas de su país.
3. La voluntad del pueblo es la base de la autoridad del poder público; esta voluntad se expresará mediante elecciones auténticas que habrán de celebrarse periódicamente, por sufragio universal e igual y por voto secreto u otro procedimiento equivalente que garantice la libertad del voto».

²⁶ «Artículo 25.-

Todos los ciudadanos gozarán, sin ninguna de las distinciones mencionadas en el artículo 2, y sin restricciones indebidas, de los siguientes derechos y oportunidades:

a) Participar en la dirección de los asuntos públicos, directamente o por medio de representantes libremente elegidos;
b) Votar y ser elegidos en elecciones periódicas, auténticas, realizadas por sufragio universal e igual y por voto secreto que garantice la libre expresión de la voluntad de los electores;
c) Tener acceso, en condiciones generales de igualdad, a las funciones públicas de su país».

²⁷ «Artículo XX. Toda persona, legalmente capacitada, tiene el derecho de tomar parte en el gobierno de su país, directamente o por medio de sus representantes, y de participar en las elecciones populares, que serán de voto secreto, genuinas, periódicas y libres».

²⁸ «Artículo 23. Derechos Políticos

1. Todos los ciudadanos deben gozar de los siguientes derechos y oportunidades:

a) de participar en la dirección de los asuntos públicos, directamente o por medio de representantes libremente elegidos;
b) de votar y ser elegidos en elecciones periódicas auténticas, realizadas por sufragio universal e igual y por voto secreto que garantice la libre expresión de la voluntad de los electores, y
c) de tener acceso, en condiciones generales de igualdad, a las funciones públicas de su país.

2. La ley puede reglamentar el ejercicio de los derechos y oportunidades a que se refiere el inciso anterior, exclusivamente por razones de edad, nacionalidad, residencia, idioma, instrucción, capacidad civil o mental, o condena, por juez competente, en proceso penal».

autoridades o los representantes, se requiere de información para ejercer un control sobre el desempeño de la función pública.

La participación política, conforme lo señalado por la Corte IDH en el caso *Castañeda Gutman vs. Estados Unidos Mexicanos*, abarca una amplia gama de actividades que las personas pueden llevar a cabo de forma individual o en grupos con el objetivo de influir en las elecciones de quienes gobernarán un Estado o tomarán decisiones sobre asuntos públicos. También implica tener un impacto en la formulación de políticas públicas gubernamentales a través de mecanismos de participación directa como referendos, plebiscitos, consultas populares o la elección de representantes democráticamente seleccionados (2008, párrs. 141 y 147).

En lo relativo a las obligaciones que surgen en relación con este derecho, la CIDH ha señalado en el caso *Oscar Elías Biscet y Otros c. Cuba* que los Estados deben respetar y garantizar la organización de todos los partidos políticos y otras asociaciones, la realización de un debate libre y la realización de elecciones generales, y con las debidas garantías, para que los resultados reflejen la voluntad popular. Adicionalmente, la CIDH ha remarcado que el libre ejercicio de este derecho implica a su vez la vigencia imprescindible de otros derechos, como la libertad de expresión, reunión y asociación (Dalla, 2011, pág. 20).

De esta manera, las nuevas tecnologías brindan una serie de posibilidades de participación en la vida política de las personas que no se hubiesen pensado de forma tradicional, como, por ejemplo, el rápido y fácil acceso a la información, poder contar con mecanismos de comunicación directa entre representantes y representados, poder agruparse en un partido político y difundir de manera masiva campañas electorales, entre otros. Sin embargo, también se plantean algunas amenazas que el uso de algoritmos, la IA y otras nuevas tecnologías generan a este derecho.

Se puede pensar, por ejemplo, en las campañas electorales en línea que se utilizan a fin de llegar a convencer a la población de dar su voto a favor de uno u otro candidato. En principio, el uso de las TIC potencia la posibilidad de acceder a este tipo de información y, en consecuencia, ejercer el derecho a la participación política. No obstante, el recurso a algoritmos y sistemas automatizados ha demostrado su capacidad para generar desinformación selectiva en la formación de la opinión política (Landa, 2023, p. 79), en tanto las empresas pueden utilizar datos almacenados con fines políticos o limitar la información a la que es posible acceder, como se señaló en el apartado previo.

Un ejemplo claro de lo mencionado anteriormente es el caso Cambridge Analytica en las elecciones presidenciales de Estados Unidos en el 2016, el cual involucró la recolección y explotación indebida de datos personales de millones de usuarios de Facebook con fines políticos. Esta consultora fue contratada por Donald Trump, quien utilizó la información de perfiles de cuentas de Facebook sin el consentimiento de los usuarios para dirigir anuncios políticos altamente personalizados al punto de manipular la decisión de los votantes a su favor, por lo que habría que preguntarse si acaso los resultados de dichas elecciones respondieron a la voluntad popular conforme al estándar desarrollado por la Corte IDH para el derecho de participación política.

Según Rodríguez-Andrés, Donald Trump obtuvo la victoria sobre Hillary Clinton al movilizar a la audiencia y destacar las vulnerabilidades de la candidata mediante el uso de las redes sociales, particularmente, de Meta (2018, p. 849). Debido a ello, la propia Clinton argumentó que Facebook había sido la causa fundamental de su derrota (Rajan, 2018). Este escándalo generó investigaciones gubernamentales, audiencias en el Congreso de los Estados Unidos y un debate público sobre la regulación de la privacidad en línea y la influencia de las redes sociales en la esfera política, generando una preocupación mundial de que las elecciones podrían

ganarlas aquellos que usan la tecnología para manipular a los votantes y no, necesariamente, porque sean los mejores candidatos o candidatas (Landa, 2023, p. 80).

Otra amenaza planteada por las nuevas tecnologías en relación con la participación política es el populismo digital o «ciberpopulismo», que consiste en propagar discursos populistas anti-democráticos a través de los medios digitales, lo que contribuye a la desinformación, producción de teorías de conspiración e incitación al odio (Walter de Santana y Archegas, 2022a). A diferencia del caso planteado líneas arriba, aquí la discusión gira en torno al contenido de los discursos divulgados de manera masiva por los propios actores políticos, el cual despierta un fuerte cuestionamiento respecto a la necesidad de plantear mínimos que permitan proteger derechos fundamentales. En ese sentido, algunas redes sociales han decidido tomar acciones para frenar este fenómeno mediante la adopción de políticas que regulan y/o moderan la publicidad política y los temas electorales.

Un ejemplo de lo anterior se encuentra en las medidas tomadas por redes sociales como Twitter, Tiktok y Telegram durante las elecciones de Brasil del 2022, contexto en el cual las redes mencionadas prohibieron todo tipo de anuncios políticos. Por su parte, Youtube prohibió videos o contenidos que indicaban que las últimas elecciones generales fueron un fraude (Walter de Santana y Archegas, 2022b). Si bien estas acciones, como se indicó, tienen como objetivo combatir el populismo, no puede ignorarse que también conllevan riesgos y afectaciones a la libertad de expresión, según se comentó en el acápite anterior.

Al respecto, el Relator Especial de las Naciones Unidas sobre la Promoción y Protección del Derecho a la Libertad de Expresión ha recomendado un marco jurídico protector de la libertad de expresión en contextos electorales que se centra en: a) promover la pluralidad en tanto los candidatos deben tener acceso a los medios de comunicación en condiciones de igualdad, así como la diversidad e independencia de los medios de comunicación; b) garantizar la transparencia en la financiación política de los partidos y de los propios medios de comunicación; y c) impulsar la rendición de cuentas que permita reparar los ataques a periodistas, activistas y candidatos públicos, así como la creación de encuestas de opinión (2014, párrs. 46-74). Agrega el Relator que cualquier limitación a lo anteriormente señalado debe encontrar una justificación que calce con los estándares desarrollados por el DIDH.

En el caso peruano destaca que, durante las elecciones políticas presidenciales y congresales de 2021, los partidos políticos suscribieron un Pacto Ético Electoral y, entre los varios compromisos que asumieron, se obligaron a usar de manera ética la IA, evitar el uso de *bots*, *trolls* o cuentas falsas para difundir propaganda electoral o posicionar sus propuestas. Sin embargo, en caso de incumplimiento, el Tribunal de Honor encargado de supervisar dicho Pacto solo podía exhortar a los responsables a honrar sus compromisos, sin ninguna consecuencia mayor a ello. En tal sentido, se destaca la necesidad de regular el uso del Internet en procesos electorales basándose en los principios de transparencia, pluralismo de la información política y electoral, así como de establecer sanciones claras a los responsables de manipular los datos e información (Landa, 2023, p. 81), a fin de asegurar el ejercicio de elecciones libres que reflejen la voluntad popular, libre de manipulaciones.

4.2. AMENAZAS A LOS DERECHOS A LA SALUD, A LA EDUCACIÓN Y AL TRABAJO

4.2.1. Derecho a la salud

El derecho a la salud es reconocido en diversos instrumentos de derechos humanos. En el SUDH se encuentra en el artículo 25²⁹ de la DUDH y en el artículo 12³⁰ del PIDESC. En el SIDH está previsto en el artículo XI³¹ de la DADDH, en el artículo 26³² de la CADH y en el artículo 10³³ del Protocolo de San Salvador.

El contenido del derecho a la salud se ha venido consolidando a partir de lo establecido por el Comité DESC en su Observación General n.º 14, en la cual sostuvo que las prestaciones médicas deben cumplir con los elementos de calidad, accesibilidad, disponibilidad y aceptabilidad. De acuerdo con dichos estándares: a) la calidad implica contar con infraestructura y personal calificado para atender las necesidades y urgencias médicas; b) la accesibilidad exige que el sistema de salud sea accesible para todas las personas, desde una perspectiva no discriminatoria, física, económica e informativa; c) la disponibilidad supone que exista una cantidad suficiente de establecimientos, bienes y servicios públicos de salud; y d) la aceptabilidad implica que se respete la ética médica y que se apliquen los enfoques de género e interculturalidad (2000, párr. 12).

²⁹ «Artículo 25.-

1. Toda persona tiene derecho a un nivel de vida adecuado que le asegure, así como a su familia, la salud y el bienestar, y en especial la alimentación, el vestido, la vivienda, la asistencia médica y los servicios sociales necesarios; tiene asimismo derecho a los seguros en caso de desempleo, enfermedad, invalidez, vejez u otros casos de pérdida de sus medios de subsistencia por circunstancias independientes de su voluntad.

2. La maternidad y la infancia tienen derecho a cuidados y asistencia especiales. Todos los niños, nacidos de matrimonio o fuera de matrimonio, tienen derecho a igual protección social».

³⁰ «Artículo 12.-

1. Los Estados Partes en el presente Pacto reconocen el derecho de toda persona al disfrute del más alto nivel posible de salud física y mental.

2. Entre las medidas que deberán adoptar los Estados Partes en el Pacto a fin de asegurar la plena efectividad de este derecho, figurarán las necesarias para:

a) La reducción de la mortalidad infantil, y el sano desarrollo de los niños;
b) El mejoramiento en todos sus aspectos de la higiene del trabajo y del medio ambiente;
c) La prevención y el tratamiento de las enfermedades epidémicas, endémicas, profesionales y de otra índole, y la lucha contra ellas;
d) La creación de condiciones que aseguren a todos asistencia médica y servicios médicos en caso de enfermedad».

³¹ «Artículo XI. Toda persona tiene derecho a que su salud sea preservada por medidas sanitarias y sociales, relativas a la alimentación, el vestido, la vivienda y la asistencia médica, correspondientes al nivel que permitan los recursos públicos y los de la comunidad».

³² «Artículo 26.- Los Estados Partes se comprometen a adoptar providencias, tanto a nivel interno como mediante la cooperación internacional, especialmente económica y técnica, para lograr progresivamente la plena efectividad de los derechos que se derivan de las normas económicas, sociales y sobre educación, ciencia y cultura, contenidas en la Carta de la Organización de los Estados Americanos, reformada por el Protocolo de Buenos Aires, en la medida de los recursos disponibles, por vía legislativa u otros medios apropiados».

³³ «Artículo 10.- Derecho a la salud

1. Toda persona tiene derecho a la salud, entendida como el disfrute del más alto nivel de bienestar físico, mental y social.

2. Con el fin de hacer efectivo el derecho a la salud los Estados Partes se comprometen a reconocer la salud como un bien público y particularmente a adoptar las siguientes medidas para garantizar este derecho:

a. La atención primaria de la salud, entendiendo como tal la asistencia sanitaria esencial puesta al alcance de todos los individuos y familiares de la comunidad;
b. La extensión de los beneficios de los servicios de salud a todos los individuos sujetos a la jurisdicción del Estado;
c. La total inmunización contra las principales enfermedades infecciosas;
d. La prevención y el tratamiento de las enfermedades endémicas, profesionales y de otra índole;
e. La educación de la población sobre la prevención y tratamiento de los problemas de salud, y
f. La satisfacción de las necesidades de salud de los grupos de más alto riesgo y que por sus condiciones de pobreza sean más vulnerables».

Los elementos del derecho a la salud también han sido recogidos por la Corte IDH en reiterada jurisprudencia sobre la materia.³⁴ En el caso *Brítez Arce y otros vs. Argentina*, este tribunal internacional destacó que la obligación de los Estados de proteger la salud se traduce en el «deber estatal de asegurar el acceso de las personas a servicios esenciales de salud» (2022a, párr. 61). Asimismo, en relación con los grupos en situación de vulnerabilidad o que se encuentran marginados, la Corte IDH ha hecho énfasis en que los Estados deben tener especial cuidado en su obligación de respeto y garantía de este derecho (2021a, párr. 185).

Los efectos positivos asociados a las nuevas tecnologías guardan relación con la ampliación de la disponibilidad y accesibilidad de los servicios de salud, permitiendo que las prestaciones médicas alcancen a un mayor número de personas. En específico, la IA y los macrodatos se usan para crear nuevas medicinas y brindar tratamientos personalizados; mientras que los dispositivos de asistencia pueden mejorar la calidad de vida y la atención sanitaria de las personas mayores (Secretario General de las Naciones Unidas, 2020a, párrs. 19-20). Sin embargo, el uso de estas tecnologías en el ámbito de la salud también puede vulnerar la intimidad de los pacientes cuando se manipulan sus datos sanitarios sensibles u otra información personal; y afectar la autonomía de las personas mayores cuando existe una dependencia excesiva a estas tecnologías (Secretario General de las Naciones Unidas, 2020a, párrs. 23-24).

La Experta Independiente sobre el disfrute de todos los derechos humanos por las personas de edad de las Naciones Unidas sostiene que, en el caso de las personas mayores, las tecnologías de apoyo y robótica han cobrado relevancia, ya que estas se utilizan para monitorear la salud y prestar asistencia en tareas diarias, como llevar alimentos o medicinas (2017, párrs. 14-15). Sin embargo, la Experta precisa que se debe garantizar que estas tecnologías no beneficien únicamente a un grupo determinado de personas, y que las ventajas que brindan partan de un enfoque integral que abarque desde la prevención de enfermedades hasta los cuidados paliativos (2017, párrs. 80-81). En adición, para evitar un acceso desigual a los avances tecnológicos, esta señaló que se deben tomar en cuenta los factores determinantes de la salud (2017, párr. 81).

La principal amenaza para este grupo poblacional es que las tecnologías pueden socavar su autonomía. La Experta enfatiza que las personas mayores con deficiencias cognitivas o aquellas que padecen demencia son las que están más expuestas al riesgo de violación de su autonomía y de ser infantilizadas, ya que las tecnologías de apoyo pueden reemplazar su voluntad y negarles la posibilidad de elegir (2017, párr. 28). En este punto, sugiere la necesidad de establecer salvaguardias para que se respeten las decisiones de las personas mayores sin que las tecnologías de apoyo o robots ejerzan coacción, por ejemplo, cuando se decide no tomar un medicamento recetado (2017, párr. 38).

Por otro lado, en el caso de los NNA, a pesar de que las tecnologías digitales pueden facilitar el acceso a servicios de salud e información relacionada y mejorar los servicios de diagnóstico y tratamiento (Comité de los Derechos del Niño, 2021, párr. 93), su funcionamiento no está exento de críticas. Por ejemplo, se cuestiona el procesamiento de datos en la búsqueda de información y servicios en línea, especialmente los relativos a salud sexual y reproductiva; y los peligros de la exposición a productos no saludables, como alcohol, drogas y tabaco, a través de la publicidad y los servicios digitales que pueden estar inapropiadamente dirigidos a niños y niñas (Comité de los Derechos del Niño, 2021, párrs. 94-97).

³⁴ Véase Corte IDH (2022, 18 de octubre). Sentencia del caso *Valencia Campos y otros vs. Bolivia* (Excepción Preliminar, Fondo, Reparaciones y Costas); Corte IDH (2021, 2 de noviembre). Sentencia del caso *Manuela y otros vs. El Salvador* (Excepciones Preliminares, Fondo, Reparaciones y Costas); Corte IDH (2018, 23 de agosto). Sentencia del caso *Cuscul Pivaral y otros vs. Guatemala* (Excepción Preliminar, Fondo, Reparaciones y Costas).

También ha sido objeto de controversia el hecho de que los avances en la salud digital acrecentan amenazas para la privacidad y la seguridad de datos, y que pueden acrecentar desigualdades preexistentes, sobre todo en agravio de los grupos más vulnerables que carecen de conectividad, como quienes viven en zonas pobres, remotas o rurales. Asimismo, la divulgación de datos de salud de personas que viven con el VIH (virus de la inmunodeficiencia humana) puede exacerbar los estigmas y las situaciones de discriminación de las que son víctimas. Igualmente, es fundamental garantizar la privacidad de los datos biométricos usados en el sistema de salud, como son las huellas digitales o los escáneres oculares. Por estas razones, se procura que los servicios de salud digital tengan una cobertura universal y que cumplan con disminuir las desigualdades, proteger la privacidad de los pacientes, así como evitar una mayor estigmatización y discriminación (Dhaliwal, 2020).

En línea con las potenciales afectaciones que las nuevas tecnologías generan en el campo de la salud, Derechos Digitales publicó en el 2020 un informe titulado *Narrativas en torno al uso de la huella digital en la salud pública*. En dicho informe, la organización cuestionó el uso de datos biométricos en el sector público de salud en Chile —el Fondo Nacional de Salud conocido con las siglas de FONASA— y en los servicios de atención primaria, pues señala que, en Chile, ninguna de las empresas que prestan los servicios de lector de huella digital presenta de manera pública un protocolo de administración o de protección de datos (2020b, p. 10).

A pesar de las amenazas descritas hacia el derecho a la salud, en América Latina y el Caribe se han identificado algunos impactos positivos en este derecho con el empleo de nuevas tecnologías. Por ejemplo, durante la pandemia por la COVID-19, la CEPAL indicó que el uso de la IA facilitó el proceso de respuesta a la crisis sanitaria, desde la etapa de detección hasta la de recuperación (2021a, p. 37). Sin embargo, se han identificado al menos dos cuestiones previas para lograr la transformación digital del sector salud: la primera es construir una infraestructura digital adecuada y brindar formación tecnológica a los miembros del sistema de salud, y la segunda es tomar en cuenta los factores socioeconómicos, culturales y geográficos que pueden negar el acceso a la salud en igualdad de condiciones (CEPAL, 2021a, pp. 36-38). Ambas cuestiones buscan evitar replicar las desigualdades y así garantizar una cobertura universal a los servicios digitales de salud. Este es uno de los desafíos pendientes en cuanto a la digitalización del sector salud en la región.

Por último, los avances de las neurotecnologías también generan como preocupación central las afectaciones que pueden tener en el derecho a la salud, ya que se trata de dispositivos tecnológicos con un carácter intrusivo en el cerebro y la actividad cerebral (Orias, 2022, p. 216). Según la UNESCO, las neurotecnologías pueden influir en el dominio y manejo que tienen las personas sobre sus estados mentales y datos cerebrales, especialmente en el caso de las interfaces cerebro-computador (BCI, por sus siglas en inglés) (2023, p. 27).

Las BCI son dispositivos que permiten que las señales provenientes del cerebro sean interpretadas como instrucciones para computadoras o máquinas, lo cual puede resultar beneficioso para aquellas personas que padecen afecciones en el sistema nervioso, como trastornos del movimiento o parálisis. Sin embargo, si las BCI son objeto de un uso no autorizado o de una manipulación maliciosa, por ejemplo, para seguir órdenes dadas por un hacker, esto tendría un impacto no solo en la autonomía de la persona, sino que también podría generar problemas de salud mental, como ansiedad y depresión (UNESCO, 2023, p. 27). Bajo este contexto, otro de los desafíos pendientes consiste en evaluar y mitigar los impactos que la aplicación de las neurotecnologías puede ocasionar en el derecho a la salud y otros derechos vinculados.

4.2.2. Derecho a la educación

El derecho a la educación está protegido por el artículo 26 de la DUDH³⁵ y el artículo 13³⁶ del PIDESC, en el marco del SUDH. Asimismo, se encuentra consagrado en el artículo XII³⁷ de la DADDH, el artículo 26 de la CADH, y el artículo 13³⁸ del Protocolo de San Salvador, en el marco del SIDH.

³⁵ «Artículo 26.-

1. Toda persona tiene derecho a la educación. La educación debe ser gratuita, al menos en lo concerniente a la instrucción elemental y fundamental. La instrucción elemental será obligatoria. La instrucción técnica y profesional habrá de ser generalizada; el acceso a los estudios superiores será igual para todos, en función de los méritos respectivos.

2. La educación tendrá por objeto el pleno desarrollo de la personalidad humana y el fortalecimiento del respeto a los derechos humanos y a las libertades fundamentales; favorecerá la comprensión, la tolerancia y la amistad entre todas las naciones y todos los grupos étnicos o religiosos, y promoverá el desarrollo de las actividades de las Naciones Unidas para el mantenimiento de la paz.

3. Los padres tendrán derecho preferente a escoger el tipo de educación que habrá de darse a sus hijos».

³⁶ «Artículo 13.-

1. Los Estados Partes en el presente Pacto reconocen el derecho de toda persona a la educación. Conviene en que la educación debe orientarse hacia el pleno desarrollo de la personalidad humana y del sentido de su dignidad, y debe fortalecer el respeto por los derechos humanos y las libertades fundamentales. Conviene asimismo en que la educación debe capacitar a todas las personas para participar efectivamente en una sociedad libre, favorecer la comprensión, la tolerancia y la amistad entre todas las naciones y entre todos los grupos raciales, étnicos o religiosos, y promover las actividades de las Naciones Unidas en pro del mantenimiento de la paz.

2. Los Estados Partes en el presente Pacto reconocen que, con objeto de lograr el pleno ejercicio de este derecho:

a) La enseñanza primaria debe ser obligatoria y asequible a todos gratuitamente;

b) La enseñanza secundaria, en sus diferentes formas, incluso la enseñanza secundaria técnica y profesional, debe ser generalizada y hacerse accesible a todos, por cuantos medios sean apropiados, y en particular por la implantación progresiva de la enseñanza gratuita;

c) La enseñanza superior debe hacerse igualmente accesible a todos, sobre la base de la capacidad de cada uno, por cuantos medios sean apropiados, y en particular por la implantación progresiva de la enseñanza gratuita;

d) Debe fomentarse o intensificarse, en la medida de lo posible, la educación fundamental para aquellas personas que no hayan recibido o terminado el ciclo completo de instrucción primaria;

e) Se debe proseguir activamente el desarrollo del sistema escolar en todos los ciclos de la enseñanza, implantar un sistema adecuado de becas, y mejorar continuamente las condiciones materiales del cuerpo docente.

3. Los Estados Partes en el presente Pacto se comprometen a respetar la libertad de los padres y, en su caso, de los tutores legales, de escoger para sus hijos o pupilos escuelas distintas de las creadas por las autoridades públicas, siempre que aquéllas satisfagan las normas mínimas que el Estado prescriba o apruebe en materia de enseñanza, y de hacer que sus hijos o pupilos reciban la educación religiosa o moral que esté de acuerdo con sus propias convicciones.

4. Nada de lo dispuesto en este artículo se interpretará como una restricción de la libertad de los particulares y entidades para establecer y dirigir instituciones de enseñanza, a condición de que se respeten los principios enunciados en el párrafo 1 y de que la educación dada en esas instituciones se ajuste a las normas mínimas que prescriba el Estado».

³⁷ «Artículo XII. Toda persona tiene derecho a la educación, la que debe estar inspirada en los principios de libertad, moralidad y solidaridad humanas.

Asimismo tiene el derecho de que, mediante esa educación, se le capacite para lograr una digna subsistencia, en mejoramiento del nivel de vida y para ser útil a la sociedad.

El derecho de educación comprende el de igualdad de oportunidades en todos los casos, de acuerdo con las dotes naturales, los méritos y el deseo de aprovechar los recursos que puedan proporcionar la comunidad y el Estado.

Toda persona tiene derecho a recibir gratuitamente la educación primaria, por lo menos».

³⁸ «Artículo 13.- Derecho a la educación

1. Toda persona tiene derecho a la educación.

2. Los Estados Partes en el presente Protocolo convienen en que la educación deberá orientarse hacia el pleno desarrollo de la personalidad humana y del sentido de su dignidad y deberá fortalecer el respeto por los derechos humanos, el pluralismo ideológico, las libertades fundamentales, la justicia y la paz. Conviene, asimismo, en que la educación debe capacitar a todas las personas para participar efectivamente en una sociedad democrática y pluralista, lograr una subsistencia digna, favorecer la comprensión, la tolerancia y la amistad entre todas las naciones y todos los grupos raciales, étnicos o religiosos y promover las actividades en favor del mantenimiento de la paz.

3. Los Estados Partes en el presente Protocolo reconocen que, con objeto de lograr el pleno ejercicio del derecho a la educación:

a. La enseñanza primaria debe ser obligatoria y asequible a todos gratuitamente;

b. La enseñanza secundaria en sus diferentes formas, incluso la enseñanza secundaria técnica y profesional, debe ser generalizada y hacerse accesible a todos, por cuantos medios sean apropiados, y en particular por la implantación progresiva de la enseñanza gratuita;

c. La enseñanza superior debe hacerse igualmente accesible a todos, sobre la base de la capacidad de cada uno, por cuantos medios sean apropiados y en particular, por la implantación progresiva de la enseñanza gratuita;

d. Se deberá fomentar o intensificar, en la medida de lo posible, la educación básica para aquellas

Este derecho es reconocido como un medio indispensable para la realización de otros derechos humanos, y tiene como propósito capacitar a todas las personas para que participen efectivamente en la sociedad y se favorezca la comprensión entre distintos grupos (Comité DESC, 1999, párrs. 1-4). De acuerdo con lo establecido por el Comité DESC en la Observación General n.º 13 (1999, párr. 6) y posteriormente tomado por la Corte IDH en la sentencia del caso *Gonzales Lluy y otros vs. Ecuador* (2015, párr. 235), los elementos de calidad, accesibilidad, disponibilidad y aceptabilidad deben ser satisfechos en todos los niveles educativos.

El Comité DESC en su Observación General n.º 13 también señala un conjunto de obligaciones generales que deben cumplir los Estados en relación con el derecho a la educación: abstenerse de dificultar o impedir el ejercicio del derecho; garantizar que el disfrute del derecho no sea obstaculizado por terceros; y adoptar medidas para que las personas y comunidades gocen de forma plena del derecho (1999, párr. 47). Dichas obligaciones internacionales también resultan aplicables en el contexto de la digitalización de la educación y, por ende, los Estados deben asumirlas efectivamente.

El uso de las tecnologías digitales en el sector de la educación debe asegurar las características esenciales de disponibilidad, accesibilidad, aceptabilidad y adaptabilidad. La Relatora Especial sobre el Derecho a la Educación de la ONU sostiene que el elemento de disponibilidad, en el marco de la educación digital, debe asegurar que los centros educativos cuenten con instalaciones informáticas y tecnologías de la información, así como con personal docente con destrezas digitales (2022, párr. 23). En cuanto a la accesibilidad, se ha considerado que la tecnología puede fomentar que los estudiantes tengan un acceso más amplio a la educación, aunque a su vez puede contribuir a la exclusión en el caso de aquellos que no están conectados o que tienen una conexión deficiente (2022, párrs. 25-26).

Asimismo, la aceptabilidad implica que la educación digital sea impartida respetando la diversidad cultural, lo que exige que sea pertinente y adecuada, así como que asegure la máxima calidad educativa posible. Para garantizar la presencia de estas características, el uso de las tecnologías debe ser objeto de evaluación, con el propósito de determinar la aceptabilidad de la educación digital que se brinda (2022, párrs. 29-30). La adaptabilidad puede verse beneficiada con la tecnología digital cuando se utiliza para adaptar la educación a las necesidades de los estudiantes y para hacer frente a situaciones de emergencia (2022, párr. 33).

Ahora bien, es importante advertir que las nuevas tecnologías presentan tanto impactos positivos como adversos en el ejercicio del derecho a la educación. Los impactos positivos en la educación se reflejan a través de la satisfacción de los elementos de accesibilidad y calidad, ya que las nuevas tecnologías ofrecen un acceso más amplio a la educación e incrementan las oportunidades y experiencias de aprendizaje entre los y las estudiantes (2022, párr. 35). Por ejemplo, el uso de medios digitales en el ámbito educativo promueve la creación de libros, cursos y materiales educativos en línea.

Sin embargo, al mismo tiempo, la ausencia de infraestructura y recursos necesarios puede generar problemas de accesibilidad y disponibilidad del derecho en el caso de las personas en situación de vulnerabilidad, como aquellas en condición de pobreza. Además, las nuevas

personas que no hayan recibido o terminado el ciclo completo de instrucción primaria;
e. Se deberán establecer programas de enseñanza diferenciada para los minusválidos a fin de proporcionar una especial instrucción y formación a personas con impedimentos físicos o deficiencias mentales.
4. Conforme con la legislación interna de los Estados Partes, los padres tendrán derecho a escoger el tipo de educación que habrá de darse a sus hijos, siempre que ella se adecúe a los principios enunciados precedentemente.
5. Nada de lo dispuesto en este Protocolo se interpretará como una restricción de la libertad de los particulares y entidades para establecer y dirigir instituciones de enseñanza, de acuerdo con la legislación interna de los Estados Partes».

tecnologías también pueden limitar el acceso a oportunidades educativas cuando acentúan las disparidades de género y no adoptan ajustes razonables para las personas con discapacidad (Secretario General de las Naciones Unidas, 2020a, párrs. 10-12). Frente a ello, con el fin de evitar exclusiones contrarias al principio de igualdad, los Estados deben garantizar que todas las personas puedan acceder en igualdad de condiciones a las nuevas tecnologías en el ámbito educativo.

Asimismo, se han identificado varios efectos negativos asociados a la digitalización de la educación. Entre estos, la Relatora Especial sobre el Derecho a la Educación de la ONU destaca la creciente participación de actores comerciales, quienes pugnan por un modelo de «desvinculación» de los centros educativos que consiste en ofrecer una serie de servicios aislados, en lugar de un único paquete educativo (2022, párr. 56). Por ejemplo, esto sucede cuando las empresas tecnológicas crean y venden material didáctico digital, plataformas educativas, cursos en línea, juegos y pruebas en línea a los centros educativos, los estudiantes y los padres de forma aislada.

La Relatora considera que el empleo de la tecnología digital también puede constituir una amenaza para el propósito de la educación presencial y el logro de resultados de aprendizaje, los cuales requieren de un proceso de interacción social mediante el que sea posible adquirir información, aptitudes emocionales y sociales (2022, párrs. 75-76). Por lo que enfatiza que las tecnologías digitales tienen solo la función de complementar la enseñanza (2022, párr. 46); y, por ende, la educación a distancia en línea nunca debe sustituir a la educación presencial.

A nivel regional, la CEPAL ha sostenido que, si bien la educación a través de medios digitales abrió oportunidades para la adaptación e innovación de los sistemas de enseñanza, también acentuó las brechas educativas en perjuicio de los estudiantes en situaciones más vulnerables, quienes obtuvieron resultados de aprendizaje deficientes en comparación con los estudiantes más privilegiados (2021a, p. 34). En respuesta a lo anterior, UNICEF (s/f) ha emitido diversos informes sobre la situación de la educación en América Latina y el Caribe durante la pandemia.

Por ejemplo, en el informe titulado *Respuesta educativa: alcanzando a los niños más vulnerables*, UNICEF señaló que uno de los desafíos más grandes era asegurar que NNA de recursos limitados, de áreas rurales, migrantes, refugiados, indígenas y con discapacidad accedan a la educación a distancia en igualdad de condiciones que el resto (2020, p. 1). En esa línea, UNICEF y UNESCO consideraron que la limitada presencia de recursos tecnológicos en los hogares fue un obstáculo para acceder a propuestas educativas durante la pandemia, por lo que resaltaron que es fundamental que la conectividad y su acceso sean temas prioritarios en las políticas educativas (2023, p. 78).

De hecho, durante la emergencia sanitaria se comprobó la falta de atención a las necesidades educativas de integrantes de pueblos indígenas, personas con discapacidad o poblaciones rurales, ya que no se identificaron medidas por parte de los Estados para facilitar el acceso digital de estos grupos; y que las políticas digitales carecieron de un enfoque de género para corregir las desigualdades en el acceso a la tecnología (UNICEF y UNESCO, 2023, p. 80). Estos hallazgos evidencian que el principal desafío para la inclusión de políticas digitales en el ámbito educativo regional consiste en cerrar las brechas educativas preexistentes; desarrollar medidas positivas para reducir las disparidades; y garantizar que los y las estudiantes en condiciones más vulnerables tengan un acceso efectivo a recursos tecnológicos que complementan su aprendizaje.

4.2.3. Derecho al trabajo

El derecho al trabajo está reconocido en el artículo 23³⁹ de la DUDH y el artículo 6⁴⁰ del PIDESC, en el marco del SUDH. Asimismo, este derecho encuentra protección en el artículo XIV⁴¹ de la DADDH, el artículo 26⁴² de la CADH, y los artículos 6⁴³ y 7⁴⁴ del Protocolo de San Salvador, en el marco del SIDH.

El Comité DESC establece en su Observación General n.º 18 que el derecho al trabajo tiene una faceta individual que se manifiesta en el derecho a condiciones de trabajo equitativas y satisfactorias, y una faceta colectiva que consiste en el derecho a formar sindicatos y a afiliarse

³⁹ «Artículo 23.-

1. Toda persona tiene derecho al trabajo, a la libre elección de su trabajo, a condiciones equitativas y satisfactorias de trabajo y a la protección contra el desempleo.
2. Toda persona tiene derecho, sin discriminación alguna, a igual salario por trabajo igual.
3. Toda persona que trabaja tiene derecho a una remuneración equitativa y satisfactoria, que le asegure, así como a su familia, una existencia conforme a la dignidad humana y que será completada, en caso necesario, por cualesquiera otros medios de protección social.
4. Toda persona tiene derecho a fundar sindicatos y a sindicarse para la defensa de sus intereses».

⁴⁰ «Artículo 6.-

1. Los Estados Partes en el presente Pacto reconocen el derecho a trabajar, que comprende el derecho de toda persona a tener la oportunidad de ganarse la vida mediante un trabajo libremente escogido o aceptado, y tomarán medidas adecuadas para garantizar este derecho.
2. Entre las medidas que habrá de adoptar cada uno de los Estados Partes en el presente Pacto para lograr la plena efectividad de este derecho deberá figurar la orientación y formación técnico profesional, la preparación de programas, normas y técnicas encaminadas a conseguir un desarrollo económico, social y cultural constante y la ocupación plena y productiva, en condiciones que garanticen las libertades políticas y económicas fundamentales de la persona humana».

⁴¹ «Artículo XIV. Toda persona tiene derecho al trabajo en condiciones dignas y a seguir libremente su vocación, en cuanto lo permitan las oportunidades existentes de empleo.

Toda persona que trabaja tiene derecho de recibir una remuneración que, en relación con su capacidad y destreza le asegure un nivel de vida conveniente para sí misma y su familia».

⁴² Véase supra, nota a pie de página número 35.

⁴³ «Artículo 6.- Derecho al trabajo

1. Toda persona tiene derecho al trabajo, el cual incluye la oportunidad de obtener los medios para llevar una vida digna y decorosa a través del desempeño de una actividad lícita libremente escogida o aceptada.
2. Los Estados Partes se comprometen a adoptar las medidas que garanticen plena efectividad al derecho al trabajo, en especial las referidas al logro del pleno empleo, a la orientación vocacional y al desarrollo de proyectos de capacitación técnico-profesional, particularmente aquellos destinados a los minusválidos. Los Estados partes se comprometen también a ejecutar y a fortalecer programas que coadyuven a una adecuada atención familiar, encaminados a que la mujer pueda contar con una efectiva posibilidad de ejercer el derecho al trabajo».

⁴⁴ «Artículo 7.- Condiciones justas, equitativas y satisfactorias de trabajo

Los Estados Partes en el presente Protocolo reconocen que el derecho al trabajo al que se refiere el artículo anterior, supone que toda persona goce del mismo en condiciones justas, equitativas y satisfactorias, para lo cual dichos Estados garantizarán en sus legislaciones nacionales, de manera particular:

- a. Una remuneración que asegure como mínimo a todos los trabajadores condiciones de subsistencia digna y decorosa para ellos y sus familias y un salario equitativo e igual por trabajo igual, sin ninguna distinción;
- b. El derecho de todo trabajador a seguir su vocación y a dedicarse a la actividad que mejor responda a sus expectativas y a cambiar de empleo, de acuerdo con la reglamentación nacional respectiva;
- c. El derecho del trabajador a la promoción o ascenso dentro de su trabajo para lo cual se tendrán en cuenta sus calificaciones, competencia, probidad y tiempo de servicio;
- d. La estabilidad de los trabajadores en sus empleos, de acuerdo con las características de las industrias y profesiones y con las causas de justa separación. En casos de despido injustificado, el trabajador tendrá derecho a una indemnización o a la readmisión en el empleo o a cualesquiera otra prestación prevista por la legislación nacional;
- e. La seguridad e higiene en el trabajo;
- f. La prohibición de trabajo nocturno o en labores insalubres o peligrosas a los menores de 18 años y, en general, de todo trabajo que pueda poner en peligro su salud, seguridad o moral. Cuando se trate de menores de 16 años, la jornada de trabajo deberá subordinarse a las disposiciones sobre educación obligatoria y en ningún caso podrá constituir un impedimento para la asistencia escolar o ser una limitación para beneficiarse de la instrucción recibida;
- g. La limitación razonable de las horas de trabajo, tanto diarias como semanales. Las jornadas serán de menor duración cuando se trate de trabajos peligrosos, insalubres o nocturnos;
- h. El descanso, el disfrute del tiempo libre, las vacaciones pagadas, así como la remuneración de los días feriados nacionales».

se libremente a ellos (2006, párr. 2). El contenido de este derecho también abarca el no ser privado injustamente del empleo, y que se respeten los derechos fundamentales del trabajador (2006, párrs. 6-8). Asimismo, siguiendo al Comité DESC, como parte de sus obligaciones frente al derecho al trabajo, los Estados asumen dos obligaciones inmediatas: garantizar su ejercicio sin ninguna discriminación, y adoptar medidas planificadas y orientadas hacia su plena realización (2006, párr. 19).

De igual manera, la Corte IDH ha desarrollado a través de su jurisprudencia el contenido del derecho al trabajo. En específico, se ha referido principalmente a su dimensión individual en las sentencias de, entre otros casos, *Lagos del Campo vs. Perú* (2017), *Spoltore vs. Argentina* (2020), *Buzos Miskitos (Lemoth Morris y otros) vs. Honduras* (2021b), *Casa Nina vs. Perú* (2021c), *Extrabajadores del Organismo Judicial vs. Guatemala* (2021d), *Nissen Pessolani vs. Paraguay* (2022b) y *Aguinaga Aillón vs. Ecuador* (2023), en las que el derecho al trabajo se manifiesta a través de la estabilidad laboral y las condiciones justas, equitativas y satisfactorias de trabajo.

Por un lado, en el caso *Lagos del Campo vs. Perú*, la Corte IDH señaló que la estabilidad laboral ofrece garantías de protección al trabajador que aseguran que su despido se realice bajo motivos justificados, y que disponga de recursos jurídicos efectivos que permitan cuestionar esta decisión (2017, párr. 150). Por otro lado, el Tribunal ha indicado que las condiciones justas, equitativas y satisfactorias de trabajo garantizan que el trabajador pueda realizar sus labores en condiciones adecuadas de seguridad, higiene y salud, previniendo accidentes de trabajo y enfermedades profesionales, lo cual resulta mucho más exigible cuando las actividades suponen riesgos importantes para la vida e integridad de las personas (2021b, párr. 75).

Al respecto, la OIT destacó en un comunicado de prensa que las nuevas tecnologías tienen el potencial para reducir la informalidad —incluida la laboral— en América Latina, aunque para lograrlo deban cerrarse múltiples brechas (2022a). En otro comunicado, la misma organización señaló que el surgimiento de nuevas tecnologías está conduciendo a la aparición de nuevas formas de trabajo (s/f). El potencial de las nuevas tecnologías para fomentar la formalización laboral puede analizarse a partir de la incorporación de TIC por parte de los Gobiernos, las empresas y la población en general, ya que permiten que las actividades económicas que ocurren en contextos informales se vuelvan más visibles e identificables⁴⁵ mientras se potencia la productividad (OIT, 2022b, p. 9).

Aunado a lo anterior, la CEPAL señaló en su informe titulado *Tecnologías digitales para un nuevo futuro* que, si bien la COVID-19 permitió acelerar los beneficios del teletrabajo, la proporción de las personas que pudieron trabajar en contextos de aislamiento social estuvo correlacionada con la estructura productiva y con las habilidades que estas tuvieran (2021a, p. 39). Si bien un trabajador medianamente calificado tiene el 67 % de posibilidad de trabajar desde casa (2021a, p. 39), el teletrabajo no es una opción para los trabajadores que no poseen conocimientos digitales o que realizan trabajos manuales.

En vista de este contexto, la CEPAL indicó que para aprovechar el potencial de las nuevas tecnologías digitales en los mercados laborales, sin profundizar en las desigualdades estructurales de la región, se requiere lo siguiente: «i) universalizar el acceso a Internet, a los dispositivos, a las aplicaciones, y a los programas de alfabetización digital; ii) desarrollar las

⁴⁵ Según la OIT, la situación confirma que identificar a la población informal es factible y que se puede lograr rápidamente usando las tecnologías de información y comunicación: «De acuerdo con el enfoque de política que emerge del estándar global en la Recomendación No. 204, la heterogeneidad en el empleo informal está relacionada al hecho que hacer una transición a la economía formal requiere múltiples intervenciones. Aunque muchas iniciativas de TIC no buscan la formalización *per se*, acortan los recorridos hacia la creación de empleos formales, el apoyo a la transición de la economía informal a la formal, y la prevención de la transición de la formalidad a la informalidad» (2022b, p. 18).

habilidades digitales y replantear los sistemas de protección social, y iii) diseñar marcos regulatorios para los mercados laborales digitalizados» (2021a, p. 40).

Ahora bien, el uso de las nuevas tecnologías durante la pandemia por la COVID-19 también ha evidenciado una serie de riesgos vinculados con la protección de otros derechos humanos. En concreto, la proliferación del teletrabajo durante este período demostró que, a pesar de ofrecer horarios flexibles y mayor productividad, tiene a la vez el potencial de interferir con la vida personal, especialmente en el caso de las mujeres. Fueron ellas quienes durante el confinamiento enfrentaron una superposición de las labores de cuidado, educación y del trabajo (BID, 2021). Como consecuencia, la pandemia generó que el nivel de participación de la mujer en el mercado laboral retrocediera más de una década en la región, pasando de un 52 % en el 2019 a un 46 % en el 2020 (CEPAL, 2021b).

Asimismo, en el contexto de la digitalización del trabajo, las nuevas tecnologías pueden también resultar discriminatorias. Por ejemplo, la Relatora Especial sobre Racismo y la Discriminación Racial de las Naciones Unidas reportó que Paraguay estaba utilizando un sistema de empleo digital que permitía la filtración de los posibles trabajadores por diferentes categorías, algunas de las cuales funcionaban como indicadores indirectos de la raza (2020a, párr. 27). Este sistema solo se encontraba disponible en español y, por ende, excluía a los pueblos indígenas que no hablan este idioma. Debido a esta barrera lingüística, la construcción de este sistema de selección de personal terminó restringiendo el acceso a los solicitantes de empleo que pertenecían a una etnia determinada.

De manera similar, en Brasil se está implementando un proyecto colaborativo entre el Gobierno nacional y la empresa Microsoft que busca reintegrar al mercado laboral a las personas desempleadas. El proyecto utiliza la IA para crear perfiles de personas desempleadas registradas en el Sistema Nacional de Empleo, y les ofrece oportunidades laborales y de formación profesional adaptadas a sus necesidades (Velasco y Venturini, 2021, p. 8). Sin embargo, los algoritmos pueden crear perfiles de trabajo basados en datos inexactos y sesgos humanos, que pueden terminar restringiendo las oportunidades de empleo para cierto grupo de personas, y es aún más riesgoso cuando se desconoce el funcionamiento del modelo algorítmico, el diseño de la toma de decisiones y si existe supervisión humana (Velasco y Venturini, 2021, pp. 21-22).

Asimismo, las plataformas digitales de trabajo caracterizan la relación contractual con los y las trabajadoras como una prestación de servicios en lugar de una relación laboral y, por ende, carecen de derechos laborales. Esto sucede a pesar de que las plataformas determinan unilateralmente, entre otros, el horario de trabajo, la remuneración, la pauta de atención al cliente y la legislación aplicable (OIT, 2021, p. 8). Mucho menos se garantiza la cobertura de seguridad social, en especial a repartidores de aplicaciones, quienes están expuestos a diversos riesgos de seguridad y salud (OIT, 2021, p. 9). En general, las personas que laboran en estas plataformas son migrantes en situación irregular; por ello, las propuestas que se planteen para abordar esta situación deben considerar sus intereses a fin de no generar instrumentos que propicien un mayor control en la relación laboral (Juan Carlos Lara, comunicación personal, 28 de septiembre de 2023).

En efecto, la regulación del trabajo en las plataformas digitales es uno de los principales desafíos en relación con las nuevas tecnologías y el derecho al trabajo. Al respecto, la CEPAL y la OIT consideran que la regulación de cada país debe estar orientada a proteger los derechos laborales y a la vez aprovechar las ventajas de las nuevas tecnologías (CEPAL, 2021c, p. 47). Adicionalmente, conforme a lo descrito en este estudio, deben generarse mecanismos para dar respuesta a la ausencia de un enfoque de género en la implementación del teletrabajo y a las formas de discriminación y sesgos presentes en la digitalización del trabajo.

A modo de conclusión sobre esta sección de amenazas que plantean las nuevas tecnologías a los derechos humanos, se debe dejar sentado que no existen diferencias en el impacto que estas tecnologías tienen en el ejercicio de los DCP, por un lado, y de los DESC, por otro. Sin embargo, es de advertirse que en la región de América Latina y el Caribe, a diferencia del norte global, existe una carencia de información que pueda proporcionar una comprensión real del efecto que tienen las nuevas tecnologías en los DESC en relación con los DCP. Ello, porque las investigaciones, inclusive de los propios órganos del SIDH, como se verá en la siguiente sección con mayor atención, se han concentrado en las amenazas y en los impactos a los DCP.

Al respecto, como bien señala María Paz (comunicación personal, 29 de septiembre de 2023), los avances de las nuevas tecnologías y su uso en el ejercicio y disfrute de los DESC en la región es una realidad desconocida en su mayoría debido a que las decisiones de los Estados de aplicar dicha tecnologías recaen, principalmente, en instrumentos de corte administrativo sin acceso público a las organizaciones y a la sociedad en general; por lo que se requiere además de la transparencia y rendición de cuentas por parte de los Estados, así como de la participación activa de las organizaciones de la sociedad civil durante todo el proceso de toma de decisión.

5. LA INCORPORACIÓN PROGRESIVA DE LAS NUEVAS TECNOLOGÍAS EN EL DERECHO INTERNACIONAL DE LOS DERECHOS HUMANOS

5.1. SISTEMA UNIVERSAL DE DERECHOS HUMANOS

5.1.1. Órganos de las Naciones Unidas

La Asamblea General de las Naciones Unidas en sus resoluciones 70/125 y 72/242 resalta los avances positivos de las tecnologías y su preocupación por los riesgos que estas presentan frente a los derechos humanos como la libertad de expresión y pluralidad de información, e insta a los Estados a que garanticen el ejercicio de derechos humanos en entornos digitales y en cumplimiento con los tratados internacionales y estándares desarrollados por el DIDH.

En septiembre de 2018, el Secretario General de las Naciones Unidas hizo público el documento *Estrategia del Secretario General de las Naciones Unidas en materia de nuevas tecnologías* (2018), cuyo objetivo central fue definir cómo la ONU apoyaría el uso de las tecnologías a fin de impulsar el logro de la Agenda 2030 para el Desarrollo Sostenible y facilitar su armonización con los valores consagrados en el sistema de la ONU. Asimismo, se hace hincapié en que dichos principios y compromisos deberán encontrarse en consonancia con la Carta de la organización, la DUDH y demás normas y estándares internacionales.

El referido documento contempla los principios y compromisos recogidos a continuación en la Tabla 2.

TABLA 2. PRINCIPIOS Y COMPROMISOS CONTEMPLADOS EN LA ESTRATEGIA DEL SECRETARIO NACIONAL DE LAS NACIONES UNIDAS EN MATERIA DE NUEVAS TECNOLOGÍAS

Principios	Compromisos
<p>Promoción y protección de valores globales.</p> <p>Fomento de la inclusión y transparencia.</p> <p>Trabajo en colaboración.</p> <p>Aprovechamiento de las capacidades y los mandatos existentes.</p> <p>Humildad y aprendizaje permanente.</p>	<p>Profundizar las capacidades internas de la ONU y su exposición a las nuevas tecnologías.</p> <p>Aumentar la comprensión, la promoción y el diálogo.</p> <p>Apoyar el diálogo sobre marcos normativos y de cooperación.</p> <p>Aumentar el apoyo de la ONU al desarrollo de la capacidad de los Gobiernos.</p>

Nota. Adaptado de Secretario General de la ONU (2018).

Es importante resaltar que la mencionada iniciativa condujo a la formación del Panel de Alto Nivel sobre la Cooperación Digital⁴⁶ en el 2018, por parte del Secretario General de las Naciones Unidas, António Guterres, con el propósito de proporcionar recomendaciones sobre cómo la comunidad internacional podría colaborar de manera efectiva para mejorar la utilización de las tecnologías digitales y reducir los riesgos asociados. El Panel culminó su mandato con la presentación del informe titulado *La era de la interdependencia digital* (2019), el cual contiene una serie de propuestas destinadas a mejorar la utilización de las tecnologías digitales y atenuar sus posibles peligros. Este informe recoge tres aspectos importantes vinculados con los derechos humanos y la acción humana que detallamos a continuación:

- El Panel instó al Secretario General a que inicie un examen en todos los organismos a fin de conocer cómo se están aplicando las normas y los tratados internacionales en materia de derechos humanos a las nuevas tecnologías y, en esa misma línea, a que se haga partícipe a la sociedad civil, a los Gobiernos, al sector privado y a la ciudadanía a expresar cómo deberían aplicarse dichos instrumentos.
- Por otro lado, el Panel exhortó a las empresas privadas responsables de redes sociales a cooperar con los Gobiernos frente a los peligros que representan las nuevas tecnologías, así como a los expertos, a la sociedad civil y a las organizaciones internacionales a estudiar de forma íntegra las preocupaciones que existen frente a riesgos reales y potenciales.

⁴⁶ El Panel estuvo conformado por Melinda Gates (Estados Unidos de América), Jack Ma (China), Mohammed Al Gergawi (Emiratos Árabes Unidos), Nikolai Astrup (Noruega), Vinton Cerf (Estados Unidos de América), Fadi Chehadé (Estados Unidos de América), Isabel Guerrero Pulgar (Chile), Marina Kaljurand (Estonia), Bogolo Kenewendo (Botswana), Akaliza Keza Ntwari (Rwanda), Marina Kolesnik (Federación de Rusia), Doris Leuthard (Suiza), Cathy Mulligan (Reino Unido), Edson Prestes (Brasil), Kira Radinsky (Israel), Nanjira Sambuli (Kenya), Sophie Soowon Eom (República de Corea), Dhananjayan Sriskandarajah (Australia) y Jean Tirole (Francia). Asimismo, el panel contó el apoyo de una pequeña secretaría, codirigida por Amandeep Singh Gill (India) y Jovan Kurbalija (Serbia).

- Finalmente, el Panel propuso algunos parámetros a la comunidad internacional para el uso de la IA. Así, indicó que el diseño y la creación de sistemas inteligentes autónomos debe permitir explicar sus decisiones y pedir cuentas de su uso a los seres humanos. Asimismo, se debía asegurar que estos sistemas cumplan las normas éticas y de ingeniería. También precisó que las decisiones de vida o muerte solo deben ser tomadas por seres humanos y no por las máquinas. Por último, pidió una cooperación digital con múltiples actores para establecer el diseño y los principios como la transparencia y la ausencia de sesgos en la creación y el uso de esos sistemas inteligentes.

Tras estas dos iniciativas, el Secretario General de las Naciones Unidas publicó la Hoja de Ruta para la Cooperación Digital (2020b), en la cual se indica cómo la comunidad internacional puede aprovechar mejor las oportunidades que ofrecen las tecnologías digitales, así como abordar los retos que estas plantean. La Hoja de Ruta se basa en las recomendaciones del Panel descritas anteriormente y las aportaciones de los Estados miembros, el sector privado, la sociedad civil, la comunidad técnica y otros grupos de interesados, y exhorta a la comunidad internacional a emprender las siguientes acciones:

TABLA 3. ACCIONES CLAVE DE LA HOJA DE RUTA PARA LA COOPERACIÓN DIGITAL

N.º	Acciones
1.	Lograr conectividad universal para el 2030.
2.	Promover los bienes públicos digitales.
3.	Garantizar la inclusión digital de todos.
4.	Fortalecer la construcción de capacidades digitales.
5.	Garantizar la protección de derechos humanos en la era digital.
6.	Apoyar a la economía mundial en materia de inteligencia artificial.
7.	Promover la confianza y la seguridad en el entorno digital.
8.	Construir una arquitectura más efectiva para la cooperación digital.

Nota. Adaptado de la Hoja de Ruta para la Cooperación Digital.

Por su parte, el Comité Asesor del Consejo de Derechos Humanos, en cumplimiento de la Resolución 41/11, emitió el informe *Impactos, oportunidades y retos que puedan entrañar las tecnologías digitales nuevas y emergentes en relación con la promoción y la protección de los derechos humanos* (2021). En dicho informe, el Comité Asesor destaca las contribuciones que las nuevas tecnologías aportan a los derechos humanos; incluye una lista de iniciativas relevantes de la ONU; y ofrece recomendaciones sobre cómo el Consejo de Derechos Humanos, sus procedimientos especiales y sus órganos subsidiarios pueden abordar de manera completa, inclusiva y práctica las oportunidades, los retos y las deficiencias en el ámbito de los derechos humanos relacionados con las tecnologías digitales nuevas y emergentes.

En el informe del ACNUDH, titulado *El derecho a la privacidad en la era digital* (2021), la entonces titular de la oficina, Michelle Bachelet, abordó el impacto del uso generalizado de la IA por parte de Estados y empresas, particularmente, en áreas como la creación de perfiles, la

toma de decisiones automatizadas y las tecnologías de aprendizaje automático, en el marco del ejercicio del derecho a la privacidad y derechos conexos. Después de proporcionar una visión general del marco legal internacional, resaltó los aspectos de la IA que pueden tener un efecto en la vida privada, y ofreció ejemplos de cómo esto afecta al derecho a la privacidad y a los derechos relacionados en cuatro áreas clave:

TABLA 4. PREOCUPACIÓN POR LOS SISTEMAS DE IA EN SECTORES CLAVE

La IA en la aplicación de la ley, la seguridad nacional, la justicia penal y la gestión de fronteras

Los Estados están incorporando sistemas de IA en la aplicación de la ley, seguridad nacional, justicia penal y gestión de fronteras. Estos sistemas utilizan algoritmos de predicción que analizan datos, incluidos antecedentes penales, informes policiales y publicaciones en redes sociales para predecir riesgos y tendencias futuras. Esto plantea preocupaciones sobre la privacidad, ya que se utilizan datos de un gran número de personas, y sobre los derechos humanos. Así, las predicciones pueden desencadenar intervenciones estatales, como detenciones, sin necesariamente justificar sospechas razonables.

La opacidad de las decisiones basadas en IA también plantea preocupaciones sobre la responsabilidad del Estado, especialmente en áreas como la lucha contra el terrorismo. Además, la tecnología de reconocimiento biométrico se está utilizando cada vez más. Ello plantea problemas de identificación errónea, discriminación y violaciones de la privacidad.

Además, las herramientas de IA que intentan deducir el estado emocional de las personas a partir de expresiones faciales también carecen de una base científica sólida y pueden socavar los derechos humanos al ser utilizadas por las autoridades públicas en contextos como controles policiales o interrogatorios.

Sistemas de IA y servicios públicos

El informe señala que la IA se está utilizando cada vez más en la prestación de servicios públicos y humanitarios con el propósito de aumentar la eficiencia y precisión. Sin embargo, se advierte que esta implementación de herramientas de IA puede tener efectos adversos en los derechos humanos si no se establecen garantías adecuadas. En particular, la IA se utiliza en servicios públicos que van desde la asistencia social hasta la atención a la infancia, basándose en grandes conjuntos de datos que a menudo provienen de entidades privadas y plantean preocupaciones sobre privacidad y sesgo en la toma de decisiones. La preocupación principal radica en la posibilidad de discriminación, especialmente hacia grupos marginados, y se ejemplifica con un caso en los Países Bajos, donde se prohibió un sistema digital de detección de fraudes debido a preocupaciones sobre la vulneración del derecho a la intimidad y la discriminación socioeconómica.

Uso de la IA en el contexto laboral

El informe destaca que cada vez más empleadores están utilizando tecnologías basadas en datos, incluidos sistemas de IA, para el seguimiento y la gestión de los trabajadores en el lugar de trabajo. Esta tendencia, acelerada por la pandemia de la COVID-19, se extiende desde el control del comportamiento relacionado con el trabajo hasta datos no relacionados con el trabajo. Esto aumenta el riesgo de fusionar datos de vigilancia en el lugar de trabajo con datos personales, lo que plantea graves preocupaciones sobre la privacidad. Además, los sistemas de IA utilizados para la gestión de personal a menudo tienen sesgos y carecen de transparencia y responsabilidad

adecuadas, lo que pone a los trabajadores en una posición vulnerable en términos de privacidad y control sobre sus datos. Las prácticas invasivas de cuantificación en el trabajo pueden forzar a los trabajadores a renunciar a su derecho a la privacidad a cambio de empleo.

La IA para la gestión de información en línea

El informe resalta que las plataformas de medios sociales utilizan sistemas de IA para tomar decisiones sobre la gestión de contenidos, lo que incluye clasificar, personalizar y aplicar restricciones de contenido. Estos sistemas pueden afectar negativamente los derechos a la privacidad y la libertad de expresión a nivel local y global, ya que la automatización y la aplicación de filtros pueden no tener en cuenta los impactos graves en estos derechos. La creación constante de vastos conjuntos de datos a partir del seguimiento en línea y la elaboración de perfiles de usuarios también plantea preocupaciones, ya que unas pocas empresas controlan perfiles de miles de millones de personas, lo que influye en la formación de opiniones y puede promover contenidos sensacionalistas y polarización. Además, los sistemas de recomendación pueden llevar a riesgos de privacidad, como la revelación de vínculos no deseados entre usuarios, y reflejan sesgos de género y racial en los resultados de búsqueda.

Nota. Adaptado de ACNUDH (2021).

Por otro lado, en el informe del ACNUDH, se examinan diversos enfoques a partir de los cuales abordar estos desafíos, y se presentan un conjunto de recomendaciones dirigidas a los Estados y a las empresas sobre la implementación de salvaguardias que prevengan y reduzcan al mínimo los efectos negativos de la IA, y permitan el pleno disfrute de los beneficios que esta puede aportar.

En el marco de la Conferencia General de la UNESCO, llevada a cabo en París del 9 al 24 de noviembre de 2021, la organización aprobó la *Recomendación sobre la Ética de la Inteligencia Artificial* (2021b). Dicha *Recomendación* estuvo motivada por

las repercusiones positivas y negativas profundas y dinámicas de la inteligencia artificial (IA) en las sociedades, el medio ambiente, los ecosistemas y las vidas humanas, en particular en la mente humana, debido en parte a las nuevas formas en que su utilización influye en el pensamiento, las interacciones y la adopción de decisiones de los seres humanos y afecta a la educación, las ciencias sociales y humanas, las ciencias exactas y naturales, la cultura y la comunicación y la información. (p. 1)

En atención a lo anterior, la *Recomendación* se planteó los objetivos que se presentan a continuación en la Tabla 5.

TABLA 5. OBJETIVOS DE LA RECOMENDACIÓN SOBRE LA ÉTICA DE LA INTELIGENCIA ARTIFICIAL

N.º	Acciones
1.	Proporcionar un marco universal de valores, principios y acciones para orientar a los Estados en la formulación de sus leyes, políticas u otros instrumentos relativos a la IA, de conformidad con el derecho internacional.
2.	Orientar las acciones de las personas, los grupos, las comunidades, las instituciones y las empresas del sector privado a fin de asegurar la incorporación de la ética en todas las etapas del ciclo de vida de los sistemas de IA.
3.	Proteger, promover y respetar los derechos humanos y las libertades fundamentales, la dignidad humana y la igualdad, incluida la igualdad de género; salvaguardar los intereses de las generaciones presentes y futuras; preservar el medio ambiente, la biodiversidad y los ecosistemas; y respetar la diversidad cultural en todas las etapas del ciclo de vida de los sistemas de IA.
4.	Fomentar el diálogo multidisciplinario y pluralista entre múltiples partes interesadas y la concertación sobre cuestiones éticas relacionadas con los sistemas de IA.
5.	Promover el acceso equitativo a los avances y los conocimientos en el ámbito de la IA y el aprovechamiento compartido de los beneficios, prestando especial atención a las necesidades y contribuciones de los países de ingreso mediano bajo, incluidos los países menos adelantados, los países en desarrollo sostenible y los pequeños Estados insulares en desarrollo.

Nota. Adaptado de UNESCO (2021b).

Con el fin de lograr el cumplimiento de los objetivos, en la *Recomendación*, se hace alusión a una serie de valores y principios diseñados para guiar el desarrollo y la implementación de la inteligencia artificial de manera ética y responsable, considerando su impacto en la sociedad y en el medio ambiente. Estos valores y principios están dirigidos a ayudar en la elaboración y aplicación de medidas de política y normas jurídicas basadas en los derechos, proporcionando orientación en el contexto del rápido desarrollo tecnológico.

TABLA 6. VALORES DE LA RECOMENDACIÓN SOBRE LA ÉTICA DE LA INTELIGENCIA ARTIFICIAL

Valores
<ul style="list-style-type: none"> • Respeto a los derechos humanos. Se destaca la importancia de respetar, proteger y promover los derechos humanos y la dignidad humana a lo largo del ciclo de vida de los sistemas de IA, sin importar la raza, el género, la edad, etc. • Prosperidad del medio ambiente. Se reconoce la necesidad de proteger y promover la prosperidad del medio ambiente y de los ecosistemas en el desarrollo de la IA. • Diversidad e inclusión. Se enfatiza la importancia de promover la diversidad y la inclusión, asegurando que los sistemas de IA sean accesibles para todas las personas, sin discriminación. • Vivir en sociedades pacíficas y justas. Se aboga por construir sociedades pacíficas y justas basadas en la interconexión y la solidaridad entre los seres humanos y la naturaleza.

Nota. Adaptado de UNESCO (2021b).

TABLA 7. PRINCIPIOS DE LA RECOMENDACIÓN SOBRE LA ÉTICA DE LA INTELIGENCIA ARTIFICIAL

Principios
<ul style="list-style-type: none"> • Proporcionalidad e inocuidad. Se insta a que los sistemas de IA sean proporcionados y seguros, evitando daños no deseados y evaluando los riesgos. • Equidad y no discriminación. Se busca promover la justicia social y la equidad, evitando la discriminación en el uso de la IA. • Sostenibilidad. Se destaca la importancia de evaluar continuamente el impacto humano, social, cultural, económico y ambiental de la IA para lograr sociedades sostenibles. • Derecho a la intimidad y protección de datos. Se enfatiza la necesidad de respetar la privacidad y proteger los datos personales en el desarrollo y uso de la IA. • Supervisión y decisión humanas. Se asegura que la responsabilidad ética y jurídica en las decisiones relacionadas con la IA recaen en las personas. • Transparencia y explicabilidad. Se aboga por la transparencia y la explicabilidad de los sistemas de IA, especialmente, cuando se toman decisiones que afectan a los derechos humanos. • Responsabilidad y rendición de cuentas. Se destaca la responsabilidad ética y jurídica de los actores de la IA y la necesidad de mecanismos de supervisión y rendición de cuentas. • Sensibilización y educación. Se promueve la educación y sensibilización pública sobre la IA y la importancia de datos, derechos humanos y ética. • Gobernanza y colaboración. Se subraya la necesidad de enfoques de gobernanza inclusivos y la colaboración entre múltiples partes interesadas en la regulación de la IA.

Nota. Adaptado de UNESCO (2021b).

La CEPAL también ha tenido la oportunidad de referirse a esta materia mediante el documento titulado *Tecnologías digitales para un nuevo futuro* (2021a), el cual tiene como objetivo impulsar una digitalización más inclusiva y sostenible en América Latina y el Caribe, que no solo acelere la recuperación económica, sino que también fomente una mayor productividad, mejores empleos y reducción de la desigualdad en la región en busca de un estado de bienestar digital.

El referido documento se divide en cuatro secciones. La primera destaca la importancia de avanzar hacia una sociedad digital sostenible en medio de la disrupción digital; la segunda analiza los efectos de la digitalización en el bienestar social y la igualdad, promoviendo el acceso universal a estas tecnologías; la tercera estudia la relación entre digitalización y productividad en diferentes sectores económicos y propone políticas para la recuperación pospandemia con transformación productiva; y, finalmente, la cuarta sección se centra en el estado de las agendas digitales regionales, especialmente en la gestión de datos, y ofrece recomendaciones para fortalecer la cooperación regional y avanzar hacia un mercado digital regional.

5.1.2. Órganos de tratados

En el marco de Naciones Unidas, varios órganos de tratados, entre ellos el Comité de Derechos Humanos, el Comité para la Eliminación de la Discriminación Racial y el Comité de DESC, han realizado importantes declaraciones y evaluaciones sobre cómo las nuevas tecnologías afectan a los derechos humanos de las personas. Los principales aportes en este sentido se encuentran sistematizados a continuación en la Tabla 8.

TABLA 8. OBSERVACIONES GENERALES SOBRE TECNOLOGÍAS

Comité de Derechos Humanos
Este órgano de expertos independientes, encargado de supervisar la implementación del PIDCP, ha destacado la importancia de garantizar que las restricciones a la libertad de expresión en línea sean necesarias y proporcionales (Observación General n.º 34, 2011, párr. 22). Asimismo, ha recalcado que los medios de expresión comprenden «los modos de expresión audiovisuales, electrónicos o de Internet, en todas sus formas» (Observación General n.º 34, 2011, párr. 12). El Comité también ha llamado la atención sobre la importancia de proteger la privacidad en el entorno digital y ha instado a los Estados a abordar las amenazas a la libertad de expresión en línea, incluida la vigilancia masiva.
Comité para la Eliminación de la Discriminación Racial
Este órgano, establecido en virtud de la Convención Internacional sobre la Eliminación de todas las Formas de Discriminación Racial (CERD), ha expresado su preocupación por la discriminación racial en línea y ha instado a los Estados a abordar este problema y garantizar que las personas no sean objeto de discriminación en Internet.
En la Observación General n.º 35 (2013), se señaló que los principios articulados sobre el discurso de odio racista desarrollados por el Comité eran aplicables incluso si el discurso se difundía a través de medios electrónicos como Internet y los sitios de redes sociales (párr. 7).

Comité de Derechos Económicos, Sociales y Culturales

Este Comité, a cargo de supervisar la implementación del PIDESC, ha abordado la importancia de garantizar el acceso universal a la educación y la información en línea, así como la necesidad de proteger los derechos de autor y la propiedad intelectual en el contexto digital.

En la Observación General n.º 25 (2020), el Comité señaló que «los Estados Partes deberían dirigir sus propios recursos y coordinar las medidas de los demás para asegurarse de que se produzca el progreso científico y que sus aplicaciones y beneficios se distribuyan y estén disponibles, especialmente para los grupos vulnerables y marginados» (párr. 16). Además, agregó que deben «eliminar la censura o las limitaciones arbitrarias al acceso a Internet, que menoscaban el acceso a los conocimientos científicos y su difusión» (párr. 42).

Comité de los Derechos del Niño

Como parte de su mandato de fiscalizar el cumplimiento de la CDN, el Comité de los Derechos del Niño ha recomendado que los Estados adopten medidas legislativas y administrativas contundentes para proteger a los niños de los contenidos perjudiciales y engañosos en el mundo digital (Observación General n.º 25, 2021, párr. 110). También ha exigido que se les proteja de cualquier forma de violencia producida en el entorno digital, como la trata de niños, la violencia de género, las agresiones en línea, los ciberataques y los conflictos informativos (Observación General n.º 25, 2021, párr. 82).

Así, en la Observación General n.º 25 relativa a los derechos de los niños en relación con el entorno digital, el Comité explicó cómo los Estados partes deben aplicar la CDN en el contexto del entorno digital, proporcionando orientación sobre las medidas normativas necesarias a fin de asegurar el cumplimiento total de las obligaciones establecidas en la CDN y sus Protocolos Facultativos. Ello, teniendo en cuenta las oportunidades, los riesgos y los desafíos relacionados con la promoción, el respeto, la protección y el ejercicio efectivo de los derechos de los niños en el entorno digital.

En general, estos órganos de tratados han subrayado la necesidad de equilibrar el uso de las nuevas tecnologías con la protección de los derechos humanos, incluida la libertad de expresión, privacidad y no discriminación, y los derechos de niñas, niños y adolescentes. También han destacado la importancia de que los Estados apliquen leyes y políticas que promuevan un entorno en línea seguro y respetuoso de los derechos humanos. Además, han hecho especial énfasis en la necesidad de una supervisión adecuada y una rendición de cuentas efectiva en el uso de la tecnología por parte de los Estados y actores privados.

5.1.3. Procedimientos especiales

Cabe destacar que la preocupación por el impacto de las nuevas tecnologías en los derechos humanos también ha sido materia de informes y comunicados de prensa por parte de los procedimientos especiales de las Naciones Unidas. A fines del siglo pasado, el Relator Especial sobre la Promoción y Protección del Derecho a la Libertad de Opinión y Expresión, Abid Husain, expresó su preocupación en torno al uso de estas nuevas fuentes por parte de algunos grupos y particulares, en particular, en lo referido al «racismo y la apología del odio, la incitación a la violencia, la pornografía (en particular, el uso de niños en la pornografía y el turismo sexual), la vida privada y la reputación, y los valores culturales o sociales» (1998, párr. 33).

Posteriormente, el sucesor de Abid Hussain en la Relatoría Especial sobre la Promoción y Protección del Derecho a la Libertad de Opinión y Expresión, Frank La Rue, fue parte de la *Declaración Conjunta del Décimo Aniversario: Los diez principales desafíos a la libre expresión en la próxima década* (2010).⁴⁷ Con relación al uso de las tecnologías, se hizo hincapié en que «el enorme potencial de Internet como instrumento de promoción de la libre circulación de la información y las ideas no se ha concretado plenamente, debido a los esfuerzos de algunos gobiernos para controlar o limitar este medio» (Desafío 9), y en que, si bien el Internet ha brindado un acceso sin precedentes a medios de información y comunicaciones, «la mayoría de ciudadanos del mundo no tiene acceso o tienen un acceso muy limitado» (Desafío 10). Cabe destacar que dichos retos han sido abordados por la Relatoría en diversos informes posteriores.⁴⁸

Tras ello, el aún Relator Frank La Rue, publicó un informe en el cual abordó las dificultades para proteger a los periodistas y la libertad de prensa en situaciones que no son de conflicto armado. Así, observó con preocupación «el hostigamiento de periodistas de Internet y bloggers, como la injerencia ilícita en sus sitios, la vigilancia de sus actividades en Internet, la aprehensión y detención arbitrarias y el bloqueo de sitios web que contienen información en que se critica a las autoridades» (Relator Especial sobre la Promoción y Protección del Derecho a la Libertad de Opinión y de Expresión de la ONU, 2012, párr. 63). Asimismo, reiteró que «el derecho a la libertad de expresión debía estar plenamente garantizado en Internet y en cualquier otro medio» (2012, párr. 64). Por lo que, de haber una limitación al ejercicio de este derecho a través de Internet, debe ajustarse también al artículo 19, párrafo 3 del PIDCP.⁴⁹

En su último informe al Consejo de Derechos Humanos, la Relatora Especial sobre la Promoción y Protección del Derecho a la Libertad de Opinión y de Expresión, Irene Khan, examinó la amenaza que representa la desinformación para los derechos humanos, las instituciones democráticas y los procesos de desarrollo (2021). Así, la Relatora destacó cómo se ha utilizado la desinformación en varios países de forma muy visible para socavar el derecho a unas elecciones libres y limpias. En ese marco, puso como ejemplo el caso de los Estados Unidos de América. Así, señala cómo «en las tres últimas citas electorales más importantes de los Estados Unidos de América se utilizaron campañas de desinformación con fines raciales para impedir el voto de las comunidades de color» (2021, párr. 24). Asimismo, condenó «el recurso al cierre de Internet para impedir o interrumpir, de forma intencional y arbitraria, el acceso a la información en línea», sosteniendo que estos «no frenan la desinformación, sino que dificultan la búsqueda de la verdad y probablemente fomentan los rumores» (2021, párr. 51).

En relación con lo anterior, el Relator Especial sobre la Libertad de Reunión Pacífica y de Asociación, Clément N. Voule, ha expresado su preocupación por el aumento de los «apagones de Internet» durante momentos democráticos críticos, tales como elecciones y protestas pacíficas (2021, párr. 2). Así, observó que estas medidas constituyen una violación del derecho de reunión pacífica, consagrado en el artículo 21 del PIDCP,⁵⁰ no debiendo considerarse como

⁴⁷ Presentada junto con el Representante para la Libertad de los Medios de Comunicación de la Organización para la Seguridad y la Cooperación en Europa, Sr. Miklos Haraszti; la Relatora Especial para la Libertad de Expresión de la Organización de Estados Americanos, señora Catalina Botero; y la Relatora Especial sobre la Libertad de Expresión y el Acceso a la Información de la Comisión Africana de Derechos Humanos y de los Pueblos, señora Faith Pansy Tlakula.

⁴⁸ Para mayor información, véase: <https://www.ohchr.org/es/special-procedures/sr-freedom-of-opinion-and-expression/annual-thematic-reports>.

⁴⁹ «Artículo 19

[...]

3. El ejercicio del derecho previsto en el párrafo 2 de este artículo [derecho a la libertad de expresión] entraña deberes y responsabilidades especiales. Por consiguiente, puede estar sujeto a ciertas restricciones, que deberán, sin embargo, estar expresamente fijadas por la ley y ser necesarias para:

a) Asegurar el respeto a los derechos o a la reputación de los demás;

b) La protección de la seguridad nacional, el orden público o la salud o la moral públicas».

⁵⁰ «Artículo 21

una restricción lícita de esta libertad fundamental. En este sentido, enfatizó que el acceso a los servicios de Internet y telefonía móvil deben mantenerse en todo momento, incluso durante tiempos de disturbios civiles (2021, párr. 2).

A través de la Resolución 28/16, aprobada por el Consejo de Derechos Humanos, se creó la Relatoría sobre el Derecho a la Privacidad, entre cuyas funciones destaca el determinar posibles obstáculos a la promoción y protección del derecho a la privacidad, y presentar propuestas y recomendaciones al Consejo de Derechos Humanos en relación con los retos presentes en la era digital. Así, al Relator Especial sobre la Privacidad «le interesan cada vez más las implicaciones para la privacidad de las siguientes esferas: i) vigilancia a gran escala; ii) utilización y conservación de datos personales; iii) bases de datos forenses de ADN; y, iv) datos abiertos y macrodatos» (ONU, s/f a). A lo largo de sus informes, la Relatoría ha expresado su preocupación por temas como el uso de las nuevas tecnologías para actividades de vigilancia gubernamental,⁵¹ el uso de datos personales por partes de las empresas,⁵² la divulgación de datos,⁵³ y el uso de información personal y no personal en el contexto de las soluciones de IA.⁵⁴ Asimismo, la Relatoría publicó el documento titulado *Principios que informan la privacidad y la protección de datos personales* (2022b).

Por otro lado, la Relatoría Especial sobre las Formas Contemporáneas del Racismo, Discriminación Racial, Xenofobia y Formas Conexas de Intolerancia ha emitido diversos informes sobre el impacto de las nuevas tecnologías en los derechos humanos. En este sentido, en el 2020, la Relatora Especial, E. Tendayi Achiume, emitió dos informes sobre la materia. En el primero, titulado *La discriminación racial y las tecnologías digitales emergentes: un análisis de los derechos humanos* (2020a), la Relatora concluye que «las tecnologías digitales emergentes agudizan y amplifican las desigualdades existentes, muchas de las cuales obedecen a motivos de raza, etnia y origen nacional» (párr. 4). Entre los motivos de preocupación, destaca la preeminencia de las «tecnologías de clasificación que diferencian, jerarquizan y categorizan» (2020a, párr. 7).

Así, por ejemplo, «los algoritmos de aprendizaje automático reproducen los sesgos incorporados en los conjuntos de datos a gran escala capaces de imitar y reproducir los sesgos implícitos de los humanos» (2020a, párr. 7). En el segundo, la Relatora resalta la forma en que se están desplegando tecnologías digitales para promover ideologías xenófobas y racialmente discriminatorias (2020b, párr. 3). Asimismo, hace hincapié en que «pese a la sensación generalizada de que las tecnologías digitales emergentes son neutrales y objetivas en su funcionamiento, la raza, el origen étnico y nacional y la ciudadanía determinan el ejercicio y disfrute de los derechos humanos en todos los campos en los que esas tecnologías hoy se aplican ampliamente» (2020b, párr. 5).

En el 2018, la Relatora Especial sobre la Violencia contra las Mujeres y las Niñas, sus Causas y sus Consecuencias, Dubravka Šimonović, emitió un informe en el que analizó la violencia en línea y la violencia facilitada por las TIC contra las mujeres y las niñas desde una perspectiva de derechos humanos (2018). Así, señaló que «cuando las mujeres y las niñas tienen acceso a Internet y lo usan, se enfrentan a modalidades y expresiones de violencia en línea que se manifiestan en una serie de formas múltiples, interrelacionadas y recurrentes de violencia por razón de género contra la mujer» (2018, párr. 14). Así, señaló que el «Internet se ha convertido

Se reconoce el derecho de reunión pacífica. El ejercicio de tal derecho sólo podrá estar sujeto a las restricciones previstas por la ley que sean necesarias en una sociedad democrática, en interés de la seguridad nacional, de la seguridad pública o del orden público, o para proteger la salud o la moral públicas o los derechos y libertades de los demás.

⁵¹ Véase A/HRC/34/60 y A/HRC/37/62.

⁵² Véase A/HRC/43/52.

⁵³ Véase A/72/540 y A/73/438.

⁵⁴ Véase A/HRC/46/37.

en un sitio en que se ejercen diversas formas de violencia contra las mujeres y las niñas, como la pornografía, los juegos sexistas y las violaciones de la intimidad» (2018, párr. 25).

Además, a través de distintos comunicados de prensa, los procedimientos especiales de las Naciones Unidas han hecho hincapié en la especial atención que ameritan las nuevas tecnologías. En este sentido, en un comunicado de prensa, los Relatores Especiales de Naciones Unidas que participaron en la Cumbre anual RightsCon enfatizaron que las violaciones de los derechos digitales permiten y aumentan la violencia en línea y fuera de línea, profundizando el conflicto, la discriminación sistémica contra grupos particulares y las crisis humanitarias, económicas y políticas en todo el mundo (ONU, 2022).

Adicionalmente, en un reciente comunicado de prensa, diversos expertos de las Naciones Unidas⁵⁵ solicitaron «mayor transparencia, supervisión y regulación para hacer frente a los efectos negativos sobre los derechos humanos de las herramientas digitales y los espacios en línea nuevos y emergentes» (ONU, 2023). En esa línea, los expertos expresaron su preocupación por la proliferación de programas espía invasivos, y de los llamados sistemas de «inteligencia artificial generativa». Asimismo, «reiteraron sus llamamientos a la cautela ante el impacto radical de las tecnologías digitales en el contexto de las crisis humanitarias, desde la recopilación de datos a gran escala —incluida la recolección de datos biométricos muy sensibles— hasta el uso de tecnologías avanzadas de vigilancia selectiva» (ONU, 2023).

5.2. SISTEMAS REGIONALES DE DERECHOS HUMANOS

5.2.1. Sistema Interamericano de Derechos Humanos

Los órganos del SIDH, la CIDH y la Corte IDH han ido reconociendo progresivamente los impactos de las nuevas tecnologías en la región de América y el Caribe. A pesar de que los estándares de protección se han centrado en los DCP, los últimos pronunciamientos de estos órganos interamericanos evidencian una tendencia hacia la garantía de los derechos sociales bajo un contexto de nuevas tecnologías digitales.

a) Los derechos humanos y las nuevas tecnologías a partir del trabajo de la CIDH

En cuanto a los derechos a la libertad de expresión y a la privacidad, la CIDH considera que los sistemas de vigilancia digital por parte de los Estados pueden constituir mecanismos que atentan contra tales derechos. Así lo resaltó la CIDH cuando se pronunció sobre la aplicación del *software* Pegasus para vigilar las actividades de periodistas y personas defensoras de derechos humanos en El Salvador (2022b) y México (2023a). En sus comunicados de prensa, la CIDH reiteró que los Estados deben limitar el empleo de las tecnologías con injerencia en los

⁵⁵ Fionnuala Ní Aoláin, Relatora Especial sobre la Promoción y la Protección de los Derechos Humanos y las Libertades Fundamentales en la Lucha contra el Terrorismo; Irene Khan, Relatora Especial sobre la Promoción y Protección del Derecho a la Libertad de Opinión y de Expresión; Aua Baldé (Presidenta Relatora), Gabriella Citroni (Vicepresidenta), Angkhana Neelapajit, Grażyna Baranowska, Ana Lorena Delgadillo Pérez, Grupo de Trabajo sobre Desapariciones Forzadas e Involuntarias; Ana Brian Nougères, Relatora Especial sobre el Derecho a la Privacidad; Mary Lawlor, Relatora Especial sobre la Situación de los Defensores de los Derechos Humanos; Clément Nyaletsossi Voule, Relator Especial sobre los Derechos a la Libertad de Reunión Pacífica y de Asociación; Pichamon Yeophantong (Presidenta), Damilola Olawuyi (Vicepresidente), Fernanda Hoppenhaym, Elżbieta Karska y Robert McCorquodale, Grupo de Trabajo sobre la cuestión de los derechos humanos y las empresas transnacionales y otras empresas; y Ashwini K. P., Relatora Especial sobre las Formas Contemporáneas de Racismo, Discriminación Racial, Xenofobia y Formas Conexas de Intolerancia; Tomoya Obokata, Relator Especial sobre las Formas Contemporáneas de la Esclavitud, incluidas sus causas y consecuencias.

derechos a la libertad de expresión y a la privacidad, y cuando ello suceda corresponde seguir los estándares internacionales de derechos humanos.

En esa línea, se requiere que estas injerencias tengan un sustento legal, se garantice la existencia de un objetivo legítimo y los principios de necesidad y proporcionalidad, y cuenten con una autorización judicial previa y supervisión permanente por parte de los órganos estatales. Asimismo, los Estados deben notificar a las personas que son objeto de vigilancia para que estas conozcan sobre la información recolectada y se manifiesten acerca del tratamiento que se dará a dicha información. Mientras los Estados incorporan dichos estándares en sus marcos normativos nacionales, la CIDH y el ACNUDH han llamado de manera conjunta a una moratoria inmediata sobre la venta, la transferencia y el empleo de esta tecnología (CIDH, 2021c).

Por otro lado, la CIDH y otros organismos internacionales han emitido instrumentos de *soft law* que abordan la relación de las nuevas tecnologías con los derechos a la libertad de expresión y de participación política. Ese es el caso de las Declaraciones Conjuntas: a) sobre la Libertad de Expresión y Elecciones en la era digital, y b) sobre la Independencia y la Diversidad de los Medios de Comunicación en la era digital. En la primera Declaración Conjunta, se sostiene que durante los períodos electorales rigen, entre otros principios, el deber de establecer marcos regulatorios que ofrezcan a las personas votantes información precisa y confiable sobre los partidos políticos, las personas candidatas y el proceso electoral en general; así como el deber de promover el acceso a otras tecnologías digitales y cerrar brechas de esta naturaleza (CIDH, 2020).

Además, en dicha Declaración se recomienda a los medios y a las plataformas digitales adoptar medidas para que los usuarios tengan acceso a distintas ideas y posiciones políticas, y que realicen los esfuerzos necesarios para combatir la desinformación, la manipulación intencionada de información y los correos no deseados durante el contexto electoral (CIDH, 2020). Por su parte, en la Declaración Conjunta sobre la Independencia y la Diversidad de los Medios de Comunicación en la era digital, la CIDH destaca un conjunto de amenazas tecnológicas que pueden configurarse como violaciones al derecho a la libertad de expresión: la vigilancia digital a medios de comunicación o periodistas; la eliminación de contenido en línea; o los ataques cibernéticos a los sistemas de comunicación digital (CIDH, 2018).

Igualmente, durante el período de sesiones del 2021, la CIDH llevó a cabo la audiencia temática *Uso de tecnologías de vigilancia y su impacto en la libertad de expresión en pandemia* (CIDH, 2021c). Durante la audiencia, las organizaciones de la sociedad civil solicitaron a la CIDH, entre otras cuestiones, que exhorte a los Estados a la ejecución de procesos de debida diligencia en materia de derechos humanos por parte de las empresas o instituciones dedicadas al diseño, al desarrollo, a la venta o a la compra de tecnologías de vigilancia; y que abra un proceso de consulta regional para establecer un conjunto de directrices que guíen la adquisición y el uso de las tecnologías de vigilancia, dirigidas a agentes policiales y de inteligencia (Article 19, 2021).

En su informe temático *Estándares para una internet libre, abierta e incluyente*, la Relatoría Especial para la Libertad de Expresión de la CIDH destaca que los derechos a la libertad de expresión y a la vida privada gozan de igual protección tanto en los medios de comunicación tradicionales como en Internet (2017, párr. 82). Asimismo, ambos derechos pueden estar sujetos a restricciones o injerencias admisibles a través de la red siempre y cuando los Estados cumplan con el test tripartito: a) prevista en la ley; b) persigue un objetivo legítimo; y c) es necesario en una sociedad democrática, es decir, cumple con los principios de idoneidad, necesidad y proporcionalidad (CIDH, 2017, párr. 155).

Asimismo, la Relatoría Especial para la Libertad de Expresión de la CIDH reconoce que el derecho a la privacidad se ha visto fuertemente impactado por el modelo de negocios de las redes sociales, que ofrece servicios sin costo a cambio de la propiedad de los datos generados por los usuarios, y que las personas no tienen poder de decisión sobre la información que comunican (2017, párr. 199). Por ello, considera fundamental la existencia de regímenes de protección de datos personales, que regulan su almacenamiento, procesamiento, uso y transferencia (2017, párr. 204). Así, los Estados deben adoptar políticas para prohibir el manejo de datos personales, salvo que exista un objetivo legítimo o se obtenga el consentimiento informado de la persona afectada (2017, párr. 205).

Por otra parte, la Relatoría Especial califica la vigilancia en la red como una interferencia en la vida privada de las personas. Bajo esta lógica, considera que todas las injerencias de esta naturaleza no son legítimas, salvo supuestos excepcionales como el terrorismo y la lucha contra la delincuencia organizada (2017, párr. 215). Ahora bien, la Relatoría Especial agrega que puede comprobarse la legitimidad de la vigilancia electrónica a través del test tripartito antes mencionado (2017, párr. 216), por lo que corresponde hacer un análisis individualizado en cada situación.

En el caso de los NNA, la Relatoría Especial para la Libertad de Expresión de la CIDH enfatiza que el acceso a Internet es un presupuesto indispensable para el ejercicio efectivo de los derechos humanos, en especial del derecho a la libertad de expresión (2019a, párr. 76). Ahora bien, ya que los NNA tienen la facilidad de expresarse libremente a través de Internet sin necesidad de intermediarios, se plantea el desafío de proteger su privacidad e imagen ante una eventual sobreexposición. Por ello, la Relatoría Especial considera que los Estados deben adoptar un marco legal que proteja su libertad de expresión y privacidad, así como garantizar que las empresas desarrollen políticas que armonicen estos derechos con la protección de la niñez (2019a, párr. 82).

En el caso de las personas de edad, los Estados deben llevar a cabo políticas de alfabetización digital para promover el uso responsable y autónomo de Internet y las tecnologías digitales, lo que resulta esencial para proteger su derecho a la igualdad y no discriminación (CIDH, 2022a, párr. 302). De hecho, la Convención Interamericana sobre Protección de Personas Mayores (2015) señala expresamente obligaciones de los Estados en relación con los derechos a la educación y a la accesibilidad y movilidad personal en el contexto digital.

Por un lado, la Convención establece que una de las obligaciones de los Estados en cuanto al derecho a la educación consiste en «[p]romover la educación y formación de la persona mayor en el uso de las TIC para minimizar la brecha digital, generacional y geográfica e incrementar la integración social y comunitaria» (artículo 20). Por otro lado, el mismo tratado indica, respecto al derecho a la accesibilidad y movilidad personal, que los Estados tienen la obligación de «[p]romover el acceso de la persona mayor a los nuevos sistemas y tecnologías de la información y las comunicaciones, incluida Internet y que estas sean accesibles al menor costo posible» (artículo 26).

Finalmente, en el marco de sus funciones de monitoreo de derechos humanos, en marzo de 2023, la CIDH realizó visitas a empresas de Internet en San Francisco (Estados Unidos) para recoger información sobre sus prácticas y políticas en materia de derechos humanos, y con el propósito de fortalecer la respuesta estatal frente a los desafíos que representan las tecnologías digitales en los derechos humanos. En este espacio, los representantes de los Estados de Brasil, Canadá, Colombia, Perú y Uruguay, quienes también participaron en las visitas, expresaron preocupaciones sobre la moderación de contenido, destacaron la importancia de Internet y las plataformas digitales para la democracia y la gestión pública, y los desafíos que

surgen de discursos estigmatizantes o permisivos con la violencia y la discriminación (CIDH, 2023c).

b) *Los derechos humanos y las nuevas tecnologías a partir del trabajo de la Corte IDH*

El órgano jurisdiccional del sistema interamericano, la Corte IDH, a su vez ha resuelto una serie de casos que aproximan la relación entre las nuevas tecnologías y los derechos a la libertad de expresión y a la vida privada a través de la interpretación de los artículos 11 y 13 de la CADH. En las sentencias de los casos *Perozo y otros vs. Venezuela* (2009a) y *Ríos y otros vs. Venezuela* (2009b), la Corte IDH ha dejado sentado que la protección de la libertad de expresión es amplia, y que no puede ser objeto de restricciones ni a través de controles gubernamentales o privados ni por medio de nuevas tecnologías; y que el Estado tiene la responsabilidad de garantizar este derecho ante eventuales restricciones a la expresión.

Asimismo, en la sentencia del caso *Escher y otros vs. Brasil* (2009c), la Corte IDH ha reconocido que el uso creciente de nuevas tecnologías pone en mayor riesgo el derecho a la privacidad, especialmente cuando se trata de interceptaciones y grabaciones telefónicas; por lo que los Estados tienen la obligación de adaptar y fortalecer las formas tradicionales de protección de este derecho (párr. 115). En este sentido, la Corte IDH consideró que las conversaciones telefónicas, como forma de comunicación, sí están protegidas por el derecho a la vida privada, a pesar de que no estén explícitamente mencionadas en el artículo 11 de la CADH, que reconoce este derecho y garantiza su protección ante injerencias de terceros (2009c, párr. 114). Por tanto, consideramos que este estándar también puede resultar aplicable para proteger la privacidad en los espacios digitales.

Por último, la Corte IDH también se ha referido al impacto de las nuevas tecnologías en los derechos laborales, analizando cómo deben actuar los Estados ante estas circunstancias. En la Opinión Consultiva OC-27/21, sobre los derechos a la libertad sindical, negociación colectiva y huelga, la Corte IDH ha precisado que los Estados tienen la obligación de actualizar sus leyes y políticas según los cambios producidos en el mercado laboral por los avances tecnológicos y tomando en cuenta la protección de los derechos laborales (2021a, párr. 202). Asimismo, la regulación del trabajo en el contexto de las nuevas tecnologías debe responder al carácter universal e irrenunciable de los derechos laborales, enfocarse en las personas y no solo en los mercados, y adoptar medidas específicas para reconocer, cuando corresponda, la condición de trabajadores y los derechos a la libertad sindical, la negociación colectiva y la huelga en la legislación nacional (2021a, párr. 209).

5.2.2. Sistema Europeo de Derechos Humanos

En el marco del SEDH, el 28 de enero de 1981, el Consejo de Europa abrió a la firma el Convenio para la Protección de Datos Personales (1981). El Convenio 108+ fue el primer instrumento internacional jurídicamente vinculante en el ámbito de la protección de datos personales. En virtud de este, se dispuso que las partes estaban en la obligación de adoptar las medidas necesarias para seguir en sus ordenamientos jurídicos internos los principios consagrados en el Convenio, y así garantizar la protección de los datos personales de sus respectivas poblaciones. En el 2001, el Consejo de Europa abrió a la firma el Protocolo Adicional del Convenio (2001), el cual obliga a las partes a crear autoridades de control que garanticen la protección efectiva de las personas en lo que respecta al tratamiento de sus datos personales.

Si bien el CEDH no aborda específicamente la regulación de las tecnologías de la información y la comunicación, el TEDH ha emitido sentencias relevantes sobre cuestiones relacionadas

con la tecnología y los derechos humanos. A continuación, en la Tabla 9, se aborda parte de dicha jurisprudencia.

TABLA 9. JURISPRUDENCIA DEL TEDH EN MATERIA DE TECNOLOGÍAS

Vigilancia y privacidad

El TEDH ha emitido sentencias que abordan la vigilancia estatal y la protección de la privacidad en la era digital. Por ejemplo, en el ya referido caso *Big Brother Watch y Otros v. Reino Unido*, el Tribunal se pronunció sobre la legalidad de la vigilancia masiva y la retención de datos de comunicaciones (TEDH, 2021).

Libertad de expresión en línea

El TEDH ha tratado casos relacionados con la libertad de expresión en el contexto de Internet y las redes sociales. Las sentencias han abordado cuestiones como la censura en línea y la responsabilidad de las plataformas en línea por el contenido generado por los usuarios.

Por ejemplo, en relación con la protección periodística en los medios digitales, se debe tener en especial consideración la sentencia del caso *Nagla v. Latvia* del 2013. En este caso, una periodista recibió correos electrónicos anónimos que señalaban una vulnerabilidad en la base de datos del Servicio Estatal de Hacienda, revelando un posible incumplimiento de medidas de austeridad. Tras verificar la información, la periodista la divulgó en su programa de televisión. Frente a ello, se inició una investigación penal y se solicitó a la periodista que revelara la identidad de la fuente anónima, a lo que ella se negó invocando su derecho a no divulgar sus fuentes.

A pesar de identificar la fuente anónima mediante la dirección IP, se realizó un registro en el domicilio de la periodista y se confiscaron sus dispositivos electrónicos. El TEDH consideró que obligar a identificar una fuente anónima podría tener un efecto disuasorio sobre la libertad de expresión, destacando que la protección de las fuentes periodísticas es parte del derecho a la información. Además, el Tribunal concluyó que la clasificación de información violaba el artículo 10 del CEDH⁵⁶ debido a la falta de autorización para capturar cualquier tipo de información y la insuficiente justificación de la efimeridad de las pruebas en cibercrímenes (TEDH, 2013).

Protección de datos personales

El TEDH ha emitido sentencias sobre la protección de datos personales y la importancia de garantizar que la recopilación y el procesamiento de datos cumplan con los estándares de privacidad.

A modo de ejemplo, en la sentencia del caso *Bărbulescu contra Rumanía* del 2017, el afectado alegó que su derecho a la privacidad, protegido por el artículo 8 de la CEDH⁵⁷, fue vulnerado por su empleador al monitorear sus comunicaciones elec-

⁵⁶ «Artículo 10. Libertad de expresión.

1. Toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o de comunicar informaciones o ideas sin que pueda haber injerencia de autoridades públicas y sin consideración de fronteras. El presente artículo no impide que los Estados sometan a las empresas de radiodifusión, de cinematografía o de televisión a un régimen de autorización previa.

2. El ejercicio de estas libertades, que entrañan deberes y responsabilidades, podrá ser sometido a ciertas formalidades, condiciones, restricciones o sanciones, previstas por la ley, que constituyan medidas necesarias, en una sociedad democrática, para la seguridad nacional, la integridad territorial o la seguridad pública, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, la protección de la reputación o de los derechos ajenos, para impedir la divulgación de informaciones confidenciales o para garantizar la autoridad y la imparcialidad del poder judicial».

⁵⁷ «Artículo 8. Derecho al respeto a la vida privada y familiar.

trónicas sin su consentimiento. En el caso referido, *Bărbulescu* había establecido una cuenta de Yahoo Messenger a solicitud de su empleador para uso laboral, pero después de tres años fue despedido al descubrirse que había utilizado la cuenta para asuntos personales. Los tribunales nacionales de Rumanía desestimaron su demanda, basándose en una directiva de la UE que prohíbe el uso de recursos de la empresa para fines personales y justificaron el monitoreo como necesario para determinar incumplimientos disciplinarios. *Bărbulescu* llevó su caso al TEDH, argumentando que el acceso y monitoreo de sus comunicaciones electrónicas violaban su derecho a la intimidad.

La sentencia del TEDH establece que la legalidad de la monitorización de las comunicaciones de los empleados debe evaluarse considerando varios factores. Entre ellos, si el trabajador fue informado previamente de la posibilidad de la monitorización, el grado de intromisión del empleador, la existencia de una razón legítima empresarial, la posibilidad de métodos de monitorización menos intrusivos, el uso que hace la empresa de los resultados de la monitorización y la presencia de salvaguardias para el empleado. En el caso de *Bărbulescu*, el TEDH le dio la razón, ya que no se determinó si el empleado había sido notificado previamente sobre la monitorización y no se consideraron las razones específicas para la monitorización ni si podrían haberse utilizado métodos menos intrusivos, entre otros aspectos. Tomando ello en consideración, el tribunal concluyó que la monitorización en ese caso no estaba legalmente justificada.

Es importante señalar que el TEDH no emite legislación, sino que interpreta y aplica la CEDH a través de sus sentencias. La legislación específica sobre tecnologías y derechos humanos puede variar en los países miembros del Consejo de Europa, que están sujetos a la CEDH. Además, la regulación de tecnologías puede abordarse a nivel nacional y de la UE.

6. BUENAS PRÁCTICAS ESTATALES Y MULTILATERALES PARA GARANTIZAR LA PROTECCIÓN DE LOS DERECHOS HUMANOS EN EL CONTEXTO DE LAS NUEVAS TECNOLOGÍAS

Al hablar de buenas prácticas en el ámbito de la regulación de nuevas tecnologías, se hace referencia a los enfoques, las políticas y las estrategias que los Estados y las organizaciones pueden adoptar para regular y gestionar de manera efectiva el impacto de las tecnologías emergentes en la sociedad y la economía. Estas prácticas se desarrollan con el fin de promover el desarrollo sostenible, la innovación responsable y la protección de los derechos y valores fundamentales en un entorno tecnológico en constante evolución.

En esa línea, la presente sección tiene como objetivo presentar las buenas prácticas que algunos Estados de la región activos en la materia han emprendido a fin de salvaguardar los derechos de sus ciudadanos en el entorno digital. Para ello, se brindará una aproximación general de las medidas legislativas y políticas públicas adoptadas para reducir los efectos perniciosos

1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.

2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás».

de las nuevas tecnologías y acortar la brecha digital. Además, se hará alusión a algunos de los avances más significativos a nivel jurisprudencial. Finalmente, cabe destacar que el motivo de la sección es brindar una mirada general de las medidas adoptadas por los Estados frente a las nuevas tecnologías. Sin embargo, no pretende ser una investigación exhaustiva en la materia.

6.1. BUENAS PRÁCTICAS ESTATALES

6.1.1. Medidas legislativas y políticas públicas

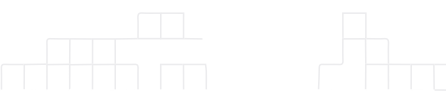
En un mundo cada vez más influenciado por avances tecnológicos, las medidas legislativas y el diseño e implementación de políticas públicas desempeñan un papel fundamental en la configuración de un entorno digital seguro, ético y eficiente. La rápida evolución de las nuevas tecnologías plantea desafíos y oportunidades únicas, y es esencial que los Gobiernos y las organizaciones adopten enfoques estratégicos para promover la innovación responsable, proteger los derechos de los ciudadanos y garantizar un desarrollo tecnológico sostenible. En este apartado, se explorarán las diversas medidas y políticas implementadas por los Estados a fin de abordar los impactos de las nuevas tecnologías en nuestra sociedad; en específico, se hará alusión al caso de Argentina, Brasil, Chile, Colombia, Costa Rica, Ecuador, México, Paraguay, Perú, Uruguay, España, Estados Unidos y Canadá.

En la actualidad, los Estados latinoamericanos se encuentran en una encrucijada en lo que respecta a las leyes y políticas públicas relacionadas con las nuevas tecnologías. La rápida adopción de innovaciones digitales en la región ha generado una creciente necesidad de regulaciones que fomenten la innovación, protejan los derechos de los ciudadanos y aborden los desafíos emergentes en el ámbito tecnológico. A continuación, en la Tabla 10 se exploran algunas de las prácticas destacadas en la regulación de tecnologías emergentes en la región latinoamericana.

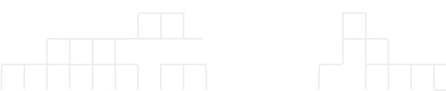
TABLA 10. LEGISLACIÓN SOBRE TECNOLOGÍAS EN LATINOAMÉRICA

País	Medida
Argentina	<p>En el 2000, Argentina aprobó la Ley de Protección de Datos Personales (Ley 25326), cuyo propósito principal fue salvaguardar la privacidad de los datos personales almacenados en archivos, registros, bases de datos y otros medios técnicos de procesamiento de datos, tanto públicos como privados, con el objetivo de garantizar el derecho al honor y a la intimidad de las personas. Este enfoque se alineó con lo establecido en el artículo 43 de la Constitución de la nación Argentina, que otorga a todas las personas el derecho de solicitar información sobre los datos que les conciernen, así como su finalidad, y les permite exigir la corrección, eliminación, confidencialidad o actualización de estos en caso de inexactitudes o discriminación.</p> <p>En el 2014, la Ley 27.078-Argentina Digital reconoció como un interés público fundamental el avance de las tecnologías de la información y las comunicaciones, las telecomunicaciones y sus recursos relacionados. Además, estableció la plena neutralidad de las redes en su artículo 1. En tiempos más recientes, el Gobierno argentino ha implementado diversas políticas públicas orientadas a las nuevas tecnologías con el objetivo de fomentar el desarrollo y la adopción de la IA en el país.</p>

Brasil	<p>En el 2014, Brasil promulgó el Marco Civil de Internet (Ley 12.965), que estableció principios, garantías, derechos y responsabilidades para el uso de Internet en el país, según se menciona en su artículo 1. Además, en el 2018, se aprobó la Ley General de Protección de Datos Personales (Ley 13.709/2018), la cual estableció regulaciones para salvaguardar la información personal de todos los ciudadanos brasileños con el propósito de proteger los derechos de libertad, privacidad y desarrollo personal. Finalmente, en el 2021, el Senado brasileño aprobó la Propuesta de Enmienda a la Constitución (PEC) 17/19, que reconoció la protección de datos personales como un derecho fundamental.</p>
Chile	<p>En 1999, Chile promulgó la Ley de Protección de la Vida Privada (Ley 19.628), la cual regula el manejo de información personal en registros o bases de datos, y establece la responsabilidad de respetar los derechos de las personas, tanto para organismos públicos como privados. Además, en el 2010, la Ley 20.453 introdujo los artículos 24 H, 24 I y 24 J en la Ley General de Telecomunicaciones chilena (Ley 18.168). Estos artículos determinaron que las empresas que brindan servicios de telecomunicaciones públicas, incluidos los proveedores de acceso a Internet, no pueden bloquear, interferir, discriminar, obstaculizar ni restringir de manera arbitraria el derecho de los usuarios de Internet a utilizar, enviar, recibir o proporcionar contenido, aplicaciones o servicios legales a través de la red. Esto estableció el principio de neutralidad en la red, como se detalla en el artículo 24 H.</p> <p>En el 2020, el Ministerio de Ciencia, Tecnología, Conocimiento e Innovación de Chile, creado en el 2018, impulsó la Política Nacional de Ciencia, Tecnología, Conocimiento e Innovación. Su objetivo fundamental es promover, comprender y aprovechar la ciencia, la tecnología, el conocimiento y la innovación para lograr un desarrollo integral y sostenible, así como mejorar la calidad de vida de la población (2020).</p>
Colombia	<p>En el 2009, Colombia promulgó la Ley 1336, que requería a los proveedores de servicios de Internet informar sobre los métodos utilizados para bloquear páginas de pornografía infantil y agregar cláusulas obligatorias en los contratos de portales de Internet que prohíban y bloqueen el contenido pornográfico que involucre a menores de edad (artículo 3). Algunos años más tarde, en el 2012, se aprobó la Ley Estatutaria 1581, que tenía como objetivo garantizar el derecho de las personas a conocer, actualizar y corregir la información recopilada sobre ellas en bases de datos o archivos (artículo 1). En el 2020, la Consejería Presidencial para Asuntos Económicos y Transformación Digital publicó el Marco Ético para la Inteligencia Artificial, un documento que establece principios para abordar los desafíos clave de la IA.</p>
Costa Rica	<p>En el 2011, Costa Rica promulgó la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales (Ley 8.968) con el objetivo de asegurar que las personas puedan ejercer su derecho a controlar la información relacionada con su vida privada. El Reglamento de esta ley establece el derecho al olvido, que implica que la retención de datos personales que puedan afectar al titular de estos no debe superar un período de diez años desde la ocurrencia de los eventos registrados (artículo 11).</p>



Ecuador	<p>En el 2008, Ecuador implementó una nueva Constitución Política que reconoció el derecho de las personas a la protección de sus datos personales, incluyendo la capacidad de otorgar su consentimiento para la «recolección, archivo, procesamiento, distribución o divulgación de dichos datos» (sección 19 del artículo 66). Luego, en el 2015, se promulgó la Ley Orgánica de Telecomunicaciones, que exigió a los proveedores de servicios de telecomunicaciones tomar las medidas necesarias para salvaguardar los datos personales de sus usuarios y abonados. Por último, en el 2021, se aprobó la Ley Orgánica de Protección de Datos Personales, que establece condiciones para la protección y el uso legítimo de los datos personales de los usuarios y define casos de vulneración de esta protección.</p>
México	<p>En el 2010, México aprobó la Ley Federal de Protección de Datos Personales en Posesión de los Particulares con el propósito de garantizar el manejo adecuado, controlado y transparente de los datos personales en manos de individuos y organizaciones privadas. Cinco años después, se implementó el Decreto por el que se Establece la Regulación en Materia de Datos Abiertos para regular la disponibilidad de datos de carácter público generados por entidades gubernamentales federales y empresas estatales para el acceso del público en general. En el 2017, se promulgó la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados con el fin de establecer pautas mínimas para el tratamiento de datos personales y facilitar los procedimientos de acceso, corrección, eliminación y oposición a través de métodos simples y rápidos. Además, el Gobierno mexicano promovió el Plan Nacional de Desarrollo 2013-2018, que incluyó objetivos como lograr un acceso universal a la cultura mediante el uso de tecnologías de la información y la comunicación, así como la creación de una Agenda Digital de Cultura en el contexto de la Estrategia Digital Nacional.</p>
Paraguay	<p>En el 2016, Paraguay promulgó la Ley de Protección de Niños, Niñas y Adolescentes contra Contenidos Nocivos de Internet (Ley 5653), con el propósito de garantizar una protección integral a los menores de edad frente a los posibles efectos negativos que pueden surgir debido a los contenidos perjudiciales presentes en Internet (artículo 1). Para alcanzar este objetivo, los proveedores de servicios de Internet están obligados a proporcionar de manera obligatoria y gratuita a sus clientes un software de código abierto que incluye sistemas para detectar, filtrar, clasificar, eliminar y bloquear contenidos dañinos.</p>
Perú	<p>En Perú, se han emitido varias leyes y políticas públicas relacionadas con las nuevas tecnologías y la protección de datos personales. En el 2002, se aprobó la Ley 27806 (Ley de Transparencia y Acceso a la Información Pública), que tiene como objetivo fomentar la transparencia gubernamental y regular el acceso a la información a través de Internet. En el 2011, se promulgó la Ley 29733 (Ley de Protección de Datos Personales), la cual garantiza el derecho a la privacidad y establece responsabilidades para las entidades que gestionan datos personales. Además, Perú ha tomado medidas para impulsar la transformación digital, como la creación del Sistema Nacional de Transformación Digital mediante el Decreto de Urgencia 006-2020, con el propósito de fortalecer la gobernabilidad democrática y el desarrollo sostenible a través de la promoción de las TIC.</p> <p>Un logro importante que destacar es la publicación en el 2022 de la Carta Peruana de Derechos Digitales, un documento de política pública respaldado por el Decreto Supremo 029-2021-PCM, que aprueba el</p>



	<p>reglamento de la Ley de Gobierno Digital, y el Decreto de Urgencia 157-2021-PCM, que aprueba el Reglamento del Decreto de Urgencia 006-2020, que establece el Sistema Nacional de Transformación Digital. Esta Carta establece 25 derechos en el contexto digital y promueve la adopción de tecnologías emergentes como la IA.</p> <p>En el 2023 se promulgó la Ley 31814, que promueve el uso de la IA en beneficio del desarrollo económico y social del país, estableciendo principios para su desarrollo y regulación bajo la supervisión de la Presidencia del Consejo de Ministros. Asimismo, en septiembre de ese mismo año, se promulgó la Ley 31878, la cual incorporó el artículo 14-A a la Constitución Política del Perú, de acuerdo con el siguiente texto: «Artículo 14-A. El Estado garantiza, a través de la inversión pública o privada, el acceso a internet libre en todo el territorio nacional, con especial énfasis en las zonas rurales, comunidades campesinas y nativas». Con esta acción, Perú se unió a la lista de países que reconocen el acceso a Internet como un derecho fundamental.</p>
Uruguay	<p>En el 2008, Uruguay aprobó la Ley de Protección de Datos Personales y Acción de Habeas Data (Ley 18.331), que establece el derecho de cualquier persona a emprender acciones legales efectivas para conocer la información personal que la afecta y que esté almacenada en bases de datos públicas o privadas. Además, esta ley permite solicitar la corrección o eliminación de dicha información en caso de errores o falsedades (artículo 37). Al año siguiente, se emitió el Decreto 451/009, que establece que el Estado tiene la obligación de almacenar los datos recopilados por la Administración Central en centros de datos seguros ubicados en territorio nacional (artículo 3). Adicionalmente, a través de los objetivos establecidos en la Agenda Uruguay Digital 2025, Uruguay busca promover la ciudadanía digital y reducir las brechas de género en el ámbito digital.</p>

En el marco europeo, España es uno de los países miembros de la UE que mayor regulación ha establecido a fin de resguardar los derechos de sus ciudadanos en entornos digitales. A lo largo de los años, se han promulgado diversas leyes en la materia; entre ellas, la Ley Orgánica de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen, la Ley Orgánica reguladora del Derecho de Rectificación, la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico, la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales, la Ley de Trabajo a Distancia, la Ley General de Telecomunicaciones, la Ley General de Comunicación Audiovisual y la propia Constitución española. Asimismo, recientemente, España aprobó y publicó una Carta de Derechos Digitales, la cual reconoce los retos que plantea la adaptación de los derechos actuales al entorno virtual y digital, y ofrece un marco de referencia para garantizar los derechos en la nueva realidad digital.

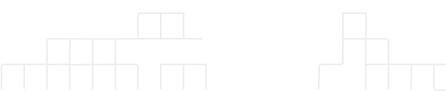


TABLA 11. LEGISLACIÓN SOBRE TECNOLOGÍAS EN ESPAÑA

Instrumento normativo	Aspectos relevantes
Ley Orgánica de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la Propia Imagen	Protege el derecho al honor, la intimidad y la propia imagen. Establece medidas para prevenir la intromisión en la vida privada y la difamación.
Ley Orgánica reguladora del Derecho de Rectificación	Garantiza el derecho de rectificación de información inexacta o difamatoria publicada en medios de comunicación.
Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico	Regula los servicios de la sociedad de la información, incluyendo el comercio electrónico y la publicidad en línea.
Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales	Regula la protección de datos personales y establece derechos digitales. Incorpora disposiciones del RGPD de la UE.
Ley de Trabajo a Distancia	Regula el trabajo a distancia, estableciendo derechos y obligaciones tanto para empleadores como para empleados.
Ley General de Telecomunicaciones	Regula el sector de las telecomunicaciones y las redes de comunicación, incluyendo la gestión del espectro radioeléctrico y la neutralidad de la red.
Ley General de Comunicación Audiovisual	Regula los servicios de comunicación audiovisual en España, incluyendo la televisión y las plataformas de contenido en línea.
Carta de Derechos Digitales	Establece derechos y garantías en el ámbito digital, como el derecho a la privacidad en línea, la neutralidad de la red y la protección de datos personales.

A nivel de Norteamérica, los Estados Unidos de América y Canadá son dos naciones líderes en el ámbito tecnológico y, a lo largo de los años, han promulgado una serie de leyes y políticas públicas destinadas a regular y aprovechar el potencial de las nuevas tecnologías. Estas medidas han sido fundamentales para abordar cuestiones cruciales como la privacidad de datos, la protección de la información personal, el desarrollo de la IA y la promoción de la innovación tecnológica en la región. A continuación, en la Tabla 12, se exploran algunas de las prácticas destacadas en la regulación de tecnologías emergentes en Norteamérica.

TABLA 12. LEGISLACIÓN SOBRE TECNOLOGÍAS EN NORTEAMÉRICA

País	Medida
Estados Unidos	<p>A nivel gubernamental, en los Estados Unidos, se han implementado diversas regulaciones con el objetivo de proteger la privacidad de los datos personales, así como la información biométrica, y garantizar un uso apropiado de la IA. En relación con la protección de datos personales, en el 2023, entraron en vigor leyes de privacidad de datos en los estados de California, Virginia, Colorado, Utah y Connecticut. En lo que respecta a la privacidad biométrica, aunque solo los estados de Illinois, Texas y Washington D.C. han promulgado leyes específicas al respecto, algunas áreas como la ciudad de Nueva York han regulado la recolección y el uso de datos biométricos (Hadgis et al, 2022). En cuanto al uso de la IA, entre el 2021 y el 2022, se observó un aumento significativo en la presentación de proyectos de ley a nivel estatal que abordaron cuestiones relacionadas con la utilización de tecnologías de reconocimiento facial por parte de las fuerzas policiales (Del Sesto y Kwon, 2023). Actualmente, los estados de Illinois, Vermont y Washington, junto con la ciudad de Nueva York, tienen disposiciones que se enfocan en aspectos particulares de la IA.</p>
Canadá	<p>A diferencia de Estados Unidos, Canadá cuenta con dos leyes de protección de datos personales a nivel federal, «the Privacy Act y the Personal Information Protection» y el «Electronic Documents Act», las cuales son aplicadas por la Oficina del Comisionado de Privacidad de Canadá. La primera ley regula el derecho de las personas a acceder y corregir la información personal que el Gobierno de Canadá tiene sobre ellas, y la segunda ley establece las reglas básicas sobre cómo las organizaciones del sector privado recopilan, usan y divulgan información personal en el curso de actividades comerciales con fines de lucro en todo el territorio canadiense. En el 2022, el Gobierno de Canadá presentó el Proyecto de Ley C-27 (Bill C-27), «An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts». El Proyecto de Ley está diseñado para actualizar la ley federal de privacidad del sector privado de Canadá (PIPEDA), crear un nuevo tribunal y proponer nuevas reglas para los sistemas de IA.</p>

Si bien aproximarnos a las buenas prácticas legislativas de los países en materia de tecnologías es vital a fin de comprender el impacto que estas han propiciado en la sociedad y en los derechos humanos de las personas, también es fundamental analizar cómo dichos impactos han sido abordados por los órganos administrativos y judiciales, y cómo producto de ello se han generado nuevos estándares de protección y limitaciones. Es por ello que en el siguiente apartado se destacarán algunas de las decisiones más importantes en la materia.

6.1.2. Jurisprudencia

La jurisprudencia sobre los impactos de las nuevas tecnologías se ha convertido en un componente esencial para configurar la evolución legal en la era digital. A medida que las tecnologías avanzan, los tribunales de todo el mundo se enfrentan a casos que plantean cuestiones

fundamentales sobre la privacidad, la propiedad intelectual, la ciberseguridad y otros temas relacionados con la tecnología. Este texto examinará algunas de las decisiones judiciales más destacadas que han delineado el camino legal en un entorno tecnológico en constante cambio.

Sobre la vulneración del derecho a la privacidad, destaca el caso *Rodríguez, María Belén c/ Google Inc. y otros/ daños y perjuicios*, sentencia del 2010 relacionada con la privacidad en línea en Argentina. Tal como señala la Corte Suprema de Justicia de la Nación (2014), la demandante presentó una demanda por daños y perjuicios contra Google Inc., luego ampliada contra Yahoo de Argentina S.R.L., alegando el uso comercial no autorizado de su imagen y la vinculación a páginas de Internet de contenido erótico o pornográfico, lo que consideraba una violación de sus derechos personales. Solicitó el cese de dicho uso y la eliminación de las vinculaciones. La sentencia de primera instancia falló a favor de la demandante, y condenó a Google a pagar \$ 100 000; y, a Yahoo, \$ 20 000. Ordenó, asimismo, la eliminación definitiva de las vinculaciones controvertidas.

Sin embargo, la Sala A de la Cámara Nacional de Apelaciones en lo Civil revocó parcialmente esta sentencia. La sentencia de segunda instancia consideró que la responsabilidad debía basarse en la negligencia demostrada después de un conocimiento efectivo de la ilicitud de un contenido y redujo las indemnizaciones, dejando sin efecto la orden de eliminación de las vinculaciones. Ambas partes presentaron recursos extraordinarios. Finalmente, la Corte Suprema de Justicia de la Nación (2014) revocó la sentencia de apelación, y rechazó la demanda en su totalidad. Argumentó que no se debe imponer una responsabilidad objetiva a los motores de búsqueda, ya que no tienen una obligación general de supervisar los contenidos en línea y que la responsabilidad debe basarse en la negligencia demostrada. También señaló que responsabilizar a los motores de búsqueda por contenidos que no crearon sería equivalente a sancionar a una biblioteca por permitir la localización de un libro dañino.

En las sentencias T-260/12 AA *en representación de su menor hija XX contra BB (2012)* y T-453/13 L *y su hijo P contra Instituto Colombiano de Bienestar Familiar y otros (2013)*, la Corte Constitucional de Colombia resolvió dos casos relativos a la protección de datos personales de menores de edad en las redes sociales. En el primer caso, la madre de una niña de cuatro años interpuso una acción de tutela contra el padre de la menor, quien creó una cuenta de Facebook a nombre de su hija, solicitando el amparo de los derechos fundamentales de su hija a la intimidad, al buen nombre y al libre desarrollo de la personalidad. A fin de resolver el caso, la Corte destacó la importancia de resguardar el principio de interés superior del niño, y de atender las recomendaciones formuladas en el «Memorándum sobre la protección de datos personales y la vida privada en redes sociales en Internet, en particular de niños, niñas y adolescentes» (Memorándum de Montevideo). En virtud de lo anterior, la Corte ordenó la cancelación de la cuenta de Facebook a nombre de la menor.

En el segundo caso, la madre de un menor de edad, a nombre propio y en representación de su hijo, interpuso acción de tutela al considerar que el Instituto Colombiano de Bienestar Familiar y la Comisaría Cuarta de Familia vulneraron los derechos de ella y su infante al permitir que se les identificara en medios masivos de comunicación. En el presente caso, la Corte Constitucional colombiana recordó que el artículo 47 del Código de la Infancia y la Adolescencia indica que los medios de comunicación, sin perjuicio de su autonomía y demás derechos, deberán «abstenerse de entrevistar, dar el nombre, divulgar datos que identifiquen o que puedan conducir a la identificación de niños, niñas y adolescentes que hayan sido víctimas, autores o testigos de un hecho delictivo» (2013, p. 6).

En ese sentido, la Corte señaló que «en caso de conflicto entre el derecho a la información y a la libertad de expresión, y el derecho a la intimidad y otros derechos fundamentales de los

menores de edad, estos últimos tienen primacía» (2013, p. 6). El tribunal señala que en numerosas ocasiones ha emitido opiniones sobre la importancia de asegurar de manera efectiva y prioritaria la realización de los derechos de aquellos que, debido a su edad temprana, requieren una protección especial. Así, señala que los menores de edad gozan de una protección reforzada, incluso cuando están involucrados en situaciones que podrían afectar su derecho a la privacidad, su integridad moral y su desarrollo. Debido a ello, la Corte ordenó al periódico que difundió la noticia que retire de la red cualquier información, reporte o datos relacionados que permitan individualizar o deducir la identidad del menor víctima de abuso sexual. De esta forma, la sentencia, de manera implícita, estableció una restricción en cuanto a los efectos de las nuevas tecnologías cuando afectan los derechos de los NNA.

Aunado a lo anterior, en la sentencia SU-458/12 (2012), la Corte concluyó que la entidad encargada de administrar las bases de datos sobre antecedentes penales vulneró el derecho al *habeas data* de los demandantes al permitir que terceros sin un interés previamente determinado conozcan la existencia de los antecedentes penales asociados a los demandantes. Asimismo, la Corte destacó que en estos casos la vulneración del *habeas data* trajo aparejada la vulneración del derecho al trabajo, y que la publicidad indiscriminada de los antecedentes penales tiene como consecuencia que las personas que tengan dichos antecedentes puedan «retomar su plan de vida en la legalidad» (2012, p. 16). Por lo que «los principios y las reglas que debe seguir el administrador de este tipo específico de bases de datos son en especial los principios de finalidad, utilidad, necesidad y circulación restringida» (2012, p. 8).

En agosto de 2023, la Corte Suprema de Chile resolvió el primer recurso presentado a nivel mundial contra Emotiv Inc.⁵⁸ por la venta y comercialización del dispositivo Insight, electroencefalograma portátil que monitorea la actividad cerebral y evalúa el estado mental de las personas. Así, en el 2022, el expresidente del Senado de Chile, Guido Girardi, interpuso un recurso de protección en contra de Emotiv Inc. ante la Corte de Apelaciones de Santiago, alegando que dicha empresa no protegía adecuadamente la privacidad de la información cerebral de sus usuarios, pues almacenaba en sus servidores informáticos los registros de la actividad cerebral (electroencefalogramas) obtenidos a través de Insight. Así, acusó la vulneración de lo dispuesto en el artículo 11 de la Ley 19.628, sobre la debida diligencia en el cuidado de datos personales a la que se encuentran obligados los responsables de registros o bases de datos personales, y a lo señalado en el artículo 13 de la referida ley sobre el derecho de las personas a la cancelación o bloqueo de sus datos personales. Ello debido a que, aun cuando la cuenta de usuario de Emotiv Inc. se encuentre cerrada, la empresa retiene información cerebral para propósitos de investigación científica e histórica. Pese a lo expuesto, la Corte de Apelaciones decidió rechazar este recurso.

Frente a ello, Girardi decidió recurrir a la Corte Suprema, la cual señaló:

[que] ante el desarrollo de nuevas tecnologías que involucran cada vez más aspectos de la persona humana [...] se debe otorgar una especial atención y cuidado en su revisión por parte del Estado, con el fin de prevenir y anticiparse a sus posibles efectos, además de proteger directamente la integridad humana en su totalidad, cuestión que incluye su privacidad y confidencialidad y los derechos propios de la integridad psíquica y del sujeto de experimentación científica (2023, p. 12).

⁵⁸ Emotiv Inc. es una empresa ubicada en San Francisco, California (Estados Unidos). Se dedica a la investigación y el desarrollo de tecnología relacionada con la neurociencia y la interfaz cerebro-computadora (BCI, por sus siglas en inglés). Emotiv ha creado dispositivos y *software* que permiten a los usuarios interactuar con computadoras y otros dispositivos electrónicos utilizando la actividad cerebral. Su tecnología se ha aplicado en una variedad de campos, como la investigación científica, la salud mental y la realidad virtual.

Por su parte, la Corte Suprema determinó que las conductas denunciadas eran contrarias al contenido protegido por los numerales 1 y 4 del artículo 19 de la Constitución Chilena, los cuales resguardan los derechos a la integridad física y psíquica y a la privacidad, ello debido a la comercialización del producto Insight «sin contar con todas las autorizaciones pertinentes, y no habiendo sido evaluado y estudiado por la autoridad sanitaria a la luz de lo expresado» (2023, p. 13). Sobre la base de lo anterior, la Corte acogió la acción «con el fin de que la autoridad sanitaria y aduanera estudie a cabalidad el dispositivo Insight» (2023, p. 13).

En el Perú, se encuentran múltiples resoluciones administrativas y judiciales que abordan cuestiones relacionadas con las tecnologías emergentes, con un enfoque específico en su repercusión en lo que respecta a la salvaguarda de la privacidad de los datos personales. En la Resolución Directoral 030-2015-JUS/DGPDP, la Dirección General de Protección de Datos Personales del Ministerio de Justicia y Derechos Humanos (2015) señaló que los creadores de contenido, especialmente los periodistas que escriben para blogs o medios de comunicación, deben limitar la inclusión de datos personales en sus artículos solo a lo estrictamente necesario para contar los hechos. Por ende, no deben añadir datos adicionales como fotos o números de identificación, a menos que estos tengan un interés público o se refieran a figuras públicas o funcionarios. En caso contrario, deben cumplir con las normativas de protección de datos.

También a nivel administrativo, mediante la Resolución Final 1050-2016-CC2 (2016), la Comisión de Protección al Consumidor del INDECOPI ha tenido oportunidad de pronunciarse sobre la responsabilidad de los aplicativos de taxis respecto a los actos cometidos por los conductores afiliados a la plataforma. En este caso, se destacó cómo incluso si los términos y las condiciones de la empresa intermediaria establecen que esta no asumirá responsabilidad por el servicio de transporte, la información proporcionada en el sitio web y la forma en que la empresa promociona sus servicios⁵⁹ pueden llevar a los consumidores a percibir que se garantiza la seguridad en la prestación del servicio de transporte contratado. En consecuencia, la empresa sería considerada responsable.

Finalmente, en el 2018, el Tribunal Constitucional del Perú se pronunció sobre las brechas digitales con motivo de la demanda de inconstitucionalidad contra la Ley 30793 (Ley que regula el gasto de publicidad del Estado peruano). Entre los argumentos de inconstitucionalidad esgrimidos por los demandantes, se señaló que el artículo 2 de la Ley 30793⁶⁰ vulneraba el derecho de acceso a la información, puesto que el acceso al servicio de Internet en el Perú no era masivo y en algunas localidades no existía posibilidad de que lo fuera por falta de infraestructura y logística (Tribunal Constitucional del Perú, 2018). Frente a ello, el Tribunal declaró la inconstitucionalidad de la ley, señalando lo siguiente:

[A]rgumentar que la difusión de la publicidad estatal pueda realizarse por redes sociales o por todos aquellos medios que implican el uso del Internet implicaría, sobre todo en el caso peruano, contar con un derecho o una libertad sin sustrato; es decir, que se tiene formalmente el derecho a obtener información, pero esa fuente será completamente inaccesible para el ciudadano. La libertad de información también genera la exigencia para el Estado de no imponer obstáculos que desalienten o impidan el libre flujo de datos relevantes para la sociedad. (2018, p. 43)

⁵⁹ En este caso, se observa que en la página web del aplicativo de taxis existía la sección «Seguridad», en la cual se señalaba lo siguiente: «De la revisión de la página web de Easy Taxi, se observa que existe una sección de “Seguridad”, en la cual se estipula lo siguiente “La seguridad es una de las principales prioridades de Easy Taxi por medio de nuestra aplicación, nuestro objetivo es conectar usuarios pasajeros y conductores de la manera más rápida y más práctica, permitiendo el traslado de los usuarios mientras disfrutan de una experiencia segura y agradable”».

⁶⁰ El cual disponía lo siguiente: «Artículo 2. Difusión libre en red digital. Dichas entidades públicas deberán igualmente suscribir cuentas en las principales aplicaciones de redes sociales, en especial, aquellas que tengan mayor difusión y número de usuarios y consignar en ellas sus comunicados, avisos y demás temas de difusión social».

En resumen, la jurisprudencia en América Latina ha desempeñado un papel fundamental en la búsqueda de un equilibrio entre la innovación tecnológica y la protección de los derechos fundamentales de los ciudadanos. A través de una serie de fallos judiciales, se ha enfocado en mitigar los efectos adversos de las nuevas tecnologías, especialmente en áreas como la privacidad, la libertad de expresión y el acceso a la información. Estos precedentes reflejan un esfuerzo por adaptar el marco legal a la era digital y garantizar que los beneficios de la tecnología sean accesibles para todos, al tiempo que se salvaguardan los valores fundamentales de la sociedad. La jurisprudencia en la región continúa evolucionando para abordar los desafíos emergentes en este ámbito en constante cambio, contribuyendo así al desarrollo de un entorno tecnológico más equitativo y justo para todos los ciudadanos.

6.1.3. Buenas prácticas multilaterales

a) Normas y directivas de la UE

La UE ha emitido diversas normas y directivas destinadas a proteger los DCP de los ciudadanos europeos en el contexto digital. En ese marco, la Carta de los Derechos Fundamentales de la UE significó uno de los primeros avances en la materia. A este respecto, el artículo 8⁶¹ de la referida Carta establece que toda persona tiene derecho a acceder y a rectificar los datos de carácter personal que la conciernan, así como a que sus datos sean protegidos, tratados de modo leal, para fines concretos y sobre la base de su consentimiento, o de un fin legítimo establecido legalmente.

Adicionalmente, señala que el respeto de lo dispuesto quedará sujeto al control de una autoridad independiente. Esto motivó que los países de la UE creen organismos nacionales responsables de proteger los datos personales de sus ciudadanos. Posteriormente, la UE adoptó el Reglamento General de Protección de Datos (Reglamento 2016/679) y la Directiva sobre Protección de Datos en el Ámbito Penal a fin de establecer mecanismos para resguardar los datos personales de los ciudadanos de los países que integran la UE.⁶²

En atención a lo anterior, cada Estado miembro de la UE tiene su propia autoridad de protección de datos que es responsable de supervisar y hacer cumplir las leyes de protección de datos en su territorio. Este es el caso de la Agencia Española de Protección de Datos, la cual tiene entre sus funciones «controlar la aplicación del Reglamento General de Protección de Datos 2016/679 y el resto de la normativa de protección de datos, así como proceder a que se aplique» y «sancionar a toda persona responsable o encargado del tratamiento con una advertencia cuando las operaciones de tratamiento previstas puedan infringir lo dispuesto en la normativa de protección de datos».⁶³ Asimismo, la UE aprobó la Ley de Servicios Digitales y la Ley de Mercados Digitales, las cuales «tienen por objeto crear un espacio digital más seguro en el que se protejan los derechos fundamentales de los usuarios y establecer unas condiciones de competencia equitativas para las empresas».

⁶¹ «Artículo 8

1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación. 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente».

⁶² Por ejemplo, el conglomerado Meta recibió una multa de 1200 millones de euros por transferir datos de usuarios de países de la UE y del Espacio Económico Europeo a los Estados Unidos, lo cual viola lo dispuesto por el artículo 46 del Reglamento.

⁶³ Para mayor información sobre las funciones y poderes de la Agencia Española de Protección de datos, revítese el siguiente enlace: <https://www.aepd.es/la-agencia/transparencia/informacion-de-caracter-institucional-organizativa-y-de-planificacion/funcion-y-poderes>.

A continuación, se brindan algunos ejemplos de cómo los Estados miembros de la UE han adaptado sus legislaciones nacionales para cumplir con las regulaciones y directivas de la UE relacionadas con las nuevas tecnologías.

TABLA 13. APLICACIÓN DE NORMATIVA DE LA UE SOBRE TECNOLOGÍAS

<p>Reglamento General de Protección de Datos (GDPR)</p>	<p>El GDPR es una regulación de la UE que entró en vigencia en mayo de 2018 y estableció normas para proteger datos personales. Los Estados miembros adaptaron sus leyes nacionales de protección de datos para estar en línea con el GDPR y crearon autoridades de protección de datos independientes. Por ejemplo, Alemania implementó la <i>Bundesdatenschutzgesetz</i> (BDSG) para complementar el GDPR.</p>
<p>Directiva de Derechos de Autor de la UE</p>	<p>La Directiva de Derechos de Autor de la UE, aprobada en el 2019, introduce reglas relacionadas con los derechos de autor en el entorno digital. Los Estados miembros deben incorporar estas reglas en sus leyes nacionales. Francia, por ejemplo, adoptó la «Loi sur le droit d’auteur et les droits voisins dans la société de l’information» para implementar esta directiva.</p>
<p>Directiva sobre Comercio Electrónico</p>	<p>La Directiva sobre Comercio Electrónico de la UE regula los servicios de la sociedad de la información y el comercio electrónico. Los Estados miembros han adaptado sus legislaciones para cumplir con esta directiva. En España, se adoptó la Ley de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI-CE) para este propósito.</p>
<p>Ley de Copyright Digital de Reino Unido</p>	<p>Aunque el Reino Unido ya no forma parte de la UE, antes de su salida, adoptó la Ley de Copyright Digital (Digital Copyright Act) para implementar regulaciones similares a las de la Directiva de Derechos de Autor de la UE.</p>

A inicios del 2023, el Parlamento Europeo, el Consejo y la Comisión proclamaron la Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital (2023a), la cual presenta el compromiso de la UE con una transformación digital protegida, segura y sostenible que sitúe a las personas en el centro, en consonancia con los valores esenciales de la UE y los derechos fundamentales. Adicionalmente, en junio de 2023, la Plenaria del Parlamento Europeo aprobó un Proyecto de Ley para regular el uso de la IA en la UE (2023b), dando inicio a la negociación con el Consejo de la Unión Europea y los representantes de los 27 países del bloque. Según el Parlamento: «Las reglas tienen como objetivo promover la adopción de una IA confiable y centrada en el ser humano y proteger la salud, la seguridad, los derechos fundamentales y la democracia de sus efectos nocivos».

El Proyecto de Ley clasifica a los sistemas de IA de acuerdo con su nivel de riesgo, el cual puede ser mínimo, limitado, alto o inaceptable. Se considerarán sistemas de IA inaceptables, y por ende prohibidos, a todos aquellos que desplieguen «técnicas subliminales» de manipulación o que influyan negativamente en grupos vulnerables; que sean utilizados por las autoridades públicas con fines de puntuación social o *social scoring*; o que realicen identificación

biométrica remota en tiempo real, salvo limitadas excepciones. Incurrir en lo anterior podría dar lugar a una multa de hasta 40 millones de euros o una cantidad equivalente al 7 % de la facturación anual mundial de una empresa, una multa mucho más severa que la dispuesta por el Reglamento General de Protección de Datos.

A lo largo de los años, el Tribunal de Justicia de la UE ha emitido diversas sentencias relacionadas con el impacto de las nuevas tecnologías en los derechos humanos. Sobre la conservación de datos, en la STJUE del 8 de abril de 2014, se declaró nula la Directiva 2006/24/CE, la cual establecía la obligación de los proveedores de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones de conservar determinados datos generados o tratados por dichos proveedores. Si bien el objetivo de la directiva es garantizar que los datos estén disponibles con fines de investigación, detección y enjuiciamiento de delito graves, esta «no establecía ningún criterio objetivo que permitiese limitar el número de personas que disponían de la autorización de acceso y utilización posterior de los datos conservados a lo estrictamente necesario teniendo en cuenta el objetivo perseguido».

En relación con el derecho al olvido,⁶⁴ destaca la STJUE del 13 de mayo de 2014 (Google Spain, S.L. y Google Inc. contra Agencia Española de Protección de Datos y Mario Costeja González). El señor Costeja, de nacionalidad española y domiciliado en España, presentó ante la Agencia Española de Protección de Datos una reclamación contra La Vanguardia Ediciones y contra Google Spain y Google Inc. En este caso, el señor Costeja solicitó que Google elimine los enlaces que vinculaban su nombre a una antigua noticia de *La Vanguardia* sobre una subasta de sus propiedades debido a deudas. Aunque la Agencia Española de Protección de Datos desestimó la reclamación contra La Vanguardia, considerando que la publicación era legalmente justificada, estimó la reclamación contra Google Spain y Google Inc., sosteniendo que los motores de búsqueda están sujetos a las regulaciones de protección de datos y pueden ser responsables de eliminar o modificar los resultados de búsqueda.

El caso llegó al Tribunal de Justicia de la Unión Europea, que determinó que, en circunstancias normales, un individuo tiene el derecho a que la información personal ya no esté vinculada a su nombre en los resultados de búsqueda, especialmente cuando no hay un interés público preponderante en mantener dicha información accesible. Sin embargo, este derecho puede ser equilibrado si existen razones específicas, como el papel público del individuo, que justifiquen mantener la información en los resultados de búsqueda. En concordancia con ello, en el artículo 17 del nuevo Reglamento General de Protección de Datos, que entró en vigor el 25 de mayo de 2018, se incluye al derecho al olvido dentro del derecho de supresión de datos personales.

b) Carta Iberoamericana de Principios y Derechos en los Entornos Digitales

En el marco de la XXVIII Cumbre Iberoamericana de Jefes y Jefes de Estado y de Gobierno, llevada a cabo en marzo de 2023, los citados países⁶⁵ adoptaron la Carta Iberoamericana de Principios y Derechos en los Entornos Digitales, la cual tiene como propósito abordar los desafíos y las oportunidades que presenta la era digital en la región iberoamericana. Algunas de las razones clave detrás de su adopción incluyen los objetivos que se presentan a continuación en la Tabla 14.

⁶⁴ El derecho al olvido se refiere al derecho de un individuo a que ciertos datos personales relacionados con ellos, que se encuentren en Internet, sean eliminados, bloqueados o excluidos de los motores de búsqueda. Esto es aplicable incluso si la información es precisa y fue inicialmente publicada de manera justificada. El derecho al olvido se ejerce cuando los datos han quedado obsoletos, ya no son relevantes debido al tiempo transcurrido o han desaparecido las razones que justificaron su tratamiento original (González, 2019, p. 57).

⁶⁵ La Carta también fue adoptada por Andorra, Bolivia, Cuba, El Salvador, España, Guatemala, Honduras, Nicaragua, Panamá, Perú, Portugal, República Dominicana y Venezuela.

TABLA 14. OBJETIVOS DE LA CARTA IBEROAMERICANA DE PRINCIPIOS Y DERECHOS EN LOS ENTORNOS DIGITALES

Protección de derechos humanos	Garantizar la protección de los derechos humanos en línea, incluyendo la libertad de expresión, la privacidad y la igualdad de género, en un entorno digital en constante evolución.
Inclusión digital	Promover la inclusión digital y garantizar que todas las personas tengan igualdad de oportunidades para acceder y participar en la sociedad de la información, independientemente de su ubicación geográfica, género, nivel de ingresos u otros factores.
Cooperación internacional	Fomentar la cooperación y colaboración entre los países iberoamericanos en asuntos relacionados con la tecnología y la sociedad de la información, reconociendo la importancia de abordar estos temas a nivel regional.
Marco regulatorio	Establecer principios y valores que guían la actuación de los países en el entorno digital y promueve la creación de marcos regulatorios que faciliten el acceso universal, equitativo y asequible a las tecnologías de la información y la comunicación.
Adaptación a la realidad digital	Reconocer la necesidad de adaptar los derechos y deberes de las personas a la nueva realidad digital, reflejando las cambiantes realidades y desafíos en el mundo digital.

Nota. Adaptado de la Carta Iberoamericana de Principios y Derechos en los Entornos Digitales.

En este sentido, la Tabla 15 presenta las secciones en las que se encuentra dividida la referida Carta.

TABLA 15. SECCIONES DE LA CARTA IBEROAMERICANA DE PRINCIPIOS Y DERECHOS EN LOS ENTORNOS DIGITALES

N.º	Secciones
1.	Centralidad de la persona. Derechos y deberes en entornos digitales
2.	Inclusión digital y conectividad
3.	Privacidad, confianza, seguridad de datos y ciberseguridad
4.	Acceso pleno a la educación, la cultura y la salud en entornos digitales inclusivos y seguros
5.	Especial atención a niñas, niños y adolescentes
6.	Participación social, económica y política en entornos digitales justos y sostenibles
7.	Administración pública digital
8.	Economía digital justa, inclusiva y segura
9.	Un abordaje de tecnologías emergentes que no renuncie a la centralidad de las personas
10.	Asistencia y cooperación iberoamericana para la transformación digital

Nota. Adaptado de la Carta Iberoamericana de Principios y Derechos en los Entornos Digitales.

En resumen, la exploración de la legislación y la jurisprudencia en materia de nuevas tecnologías en Latinoamérica, Norteamérica y Europa, junto con el enfoque en las regulaciones y decisiones de la UE y la reciente Carta Iberoamericana de Principios y Derechos en los Entornos Digitales, nos brinda una visión amplia y enriquecedora de cómo las naciones y regiones están respondiendo a los desafíos y a las oportunidades que plantean las tecnologías emergentes. A medida que estas jurisdicciones continúan evolucionando para adaptarse a un entorno digital en constante cambio, queda claro que la interacción entre la ley y la innovación tecnológica desempeñará un papel crucial en el futuro. En este sentido, el equilibrio entre la promoción de la innovación y la protección de los derechos individuales seguirá siendo un tema central en los debates legales en todo el mundo.

7. CONCLUSIONES Y RECOMENDACIONES

A lo largo de la presente investigación, se han precisado algunas de las amenazas que las nuevas tecnologías plantean en el ejercicio y disfrute de los derechos humanos de las personas, y se ha insistido en la necesidad de que el DIDH avance de forma paralela al desarrollo tecnológico. Así, se ha señalado que las amenazas a la privacidad, libertad de expresión y participación política se enfocan en la recopilación masiva de datos, la vigilancia estatal sin salvaguardas efectivas ni supervisión independiente, el uso de IA y Big Data que plantea desafíos éticos y de derechos humanos. Asimismo, se ha desarrollado la personalización del contenido, la censura y el «ciberpatrullaje» como riesgos para la libertad de expresión. En el ámbito político, resalta la manipulación de la opinión política, el populismo digital y la necesidad de marcos legales claros para garantizar la libre voluntad popular y promover la transparencia en la política en línea.

En el ámbito de la salud, se resaltó el riesgo para la privacidad y autonomía de los pacientes, especialmente en grupos vulnerables, además de las desigualdades en el acceso a la tecnología médica que podrían agravar disparidades en la atención y la discriminación por exposición de datos. En educación se señaló que, si bien la tecnología puede mejorar el acceso, también puede amplificar las brechas de calidad y acceso, excluyendo a aquellos sin recursos digitales y generando desigualdades de género. En cuanto al trabajo, se desarrolló que las nuevas tecnologías pueden excluir a personas sin habilidades digitales, resultando en trabajos precarios y falta de protección social, especialmente en plataformas digitales y para trabajadores migrantes.

Ahora bien, frente a las amenazas desarrolladas se presenta una tendencia a reconocer la necesidad de regular el uso de las nuevas tecnologías, la cual se refleja también en las respuestas propuestas de manera progresiva por el DIDH. Si bien los tratados internacionales de derechos humanos vigentes a la fecha fueron redactados sin contemplar las implicancias de las nuevas tecnologías en la vida de los seres humanos, se reconoce la importante labor del DIDH, en respuesta a lo anterior, mediante la aplicación de la interpretación dinámica de dichos tratados y la creación de instrumentos de soft law, lo que ha favorecido su adaptación a los desafíos cambiantes y complejos que plantea la era digital, así como promover un equilibrio adecuado entre la innovación tecnológica y la salvaguarda de los derechos humanos.

Bajo esa lógica, el DIDH ha reconocido que los derechos humanos también deben ser protegidos en línea y, basándose en ello, ha desarrollado una serie de estándares, principios y jurisprudencia relevantes para abordar los desafíos que genera el uso de nuevas tecnologías. Asimismo, a través de las distintas labores de los organismos internacionales, se ha promovido la participación de la sociedad civil y el diálogo internacional que facilita el trabajo colaborativo entre los Estados y otros actores relevantes. De igual forma se han desarrollado recomendaciones dirigidas a las empresas de tecnología en la creación y el funcionamiento de nuevas tecnologías, así como investigaciones y documentación de abusos en líneas que ha dado lugar a aumentar la conciencia sobre las amenazas a los derechos humanos. Sin embargo, como hemos dado cuenta en el presente informe, los alcances de la labor del DIDH encuentran importantes limitaciones para la protección efectiva de los derechos en el contexto digital.

En primer lugar, el funcionamiento de la tecnología no se limita a fronteras nacionales, lo que dificulta la aplicación coherente de normas de derechos humanos en todo el mundo, y a ello le sumamos la evolución rápida de las nuevas tecnologías que supera la capacidad de respuesta pronta y efectiva para estar «al día» con los avances tecnológicos. Adicionalmente, el DIDH se enfrenta a serios desafíos técnicos al momento de identificar y responder ante las violaciones de derechos humanos en línea, lo que aplica también en sede interna por falta de conocimientos en los sistemas judiciales.

En segundo lugar, la normativa y los estándares desarrollados por el DIDH están enfocados principalmente en garantizar los DCP, por lo que queda un gran desafío cuando se trata de DESC. Inclusive los estándares internacionales que existen sobre DCP no son aplicados por los Estados, cuyas acciones están orientadas por la falta de transparencia y rendición de cuentas. Asimismo, el DIDH debe hacer frente a las resistencias de cumplimiento de los estándares internacionales de derechos humanos por parte de las empresas, en tanto, como señala César Landa (comunicación personal, sábado 23 de septiembre de 2023) en referencia a las empresas de tecnología que tienen un considerable control sobre la creación y el manejo de las nuevas tecnologías y están orientadas al cumplimiento de fines comerciales, antes que de protección de derechos.

Abordar las limitaciones señaladas requiere de esfuerzos colaborativos a nivel nacional e internacional para aplicar un enfoque transversal del DIDH en relación con las nuevas tecnologías que permitan adaptar y fortalecer la normativa ya existente. Ello implica que el DIDH debe cumplir el rol de acompañar el avance de las nuevas tecnologías y constituirse en la base para la creación, el funcionamiento e incluso la prohibición del uso de nuevas tecnologías a fin de mitigar los riesgos y prevenir que ocurran (María Paz, comunicación personal, 29 de septiembre de 2023). Para ello, se requiere de mecanismos precisos como, por ejemplo, las evaluaciones de riesgos previo al funcionamiento de nuevos dispositivos de IA, o la creación de instituciones supervisoras que puedan asegurar la transparencia y rendición de cuentas por parte de los Estados y del sector privado en el uso de las nuevas tecnologías, así como la participación activa de la sociedad civil.

En virtud de lo expuesto y en atención a que el presente trabajo está centrado en las obligaciones que se desprenden del DIDH, planteamos las siguientes recomendaciones a los Estados:

1. Revisar y actualizar sus leyes y prácticas nacionales para asegurarse de que estén en conformidad con los estándares internacionales de derechos humanos en el contexto de las nuevas tecnologías. Esto incluye la adopción de leyes de protección de datos personales, leyes de privacidad en línea y leyes que prohíban la vigilancia masiva y arbitraria.
2. Aplicar un enfoque de derechos humanos, de manera transversal, en la creación de políticas públicas relativas al uso de las nuevas tecnologías. Asimismo, deben desarrollar marcos regulatorios para las redes sociales e impulsar acciones de autorregulación para el sector empresarial, especialmente dedicado a las nuevas tecnologías.
3. Garantizar que las leyes y regulaciones relacionadas con la tecnología no restrinjan indebidamente la libertad de expresión en línea. Deben permitir un espacio en línea abierto, libre e incluyente para la expresión de opiniones y el intercambio de información.
4. Crear mecanismos de transparencia en la recopilación y el uso de datos personales, garantizar la rendición de cuentas de las empresas y los organismos gubernamentales que manejan estos datos. Esto incluye las actividades relacionadas con el «ciberpatrullaje» y la vigilancia digital, así como la disponibilidad de mecanismos de quejas y recursos legales efectivos.
5. Limitar la vigilancia estatal en línea a lo estrictamente necesario y solo en casos legítimos. Dichas prácticas deben estar sujetas a autorización judicial previa, ser necesaria y proporcional, y estar sujeta a supervisión independiente. Las personas defensoras de derechos humanos y periodistas que operan en el entorno digital deben recibir una especial protección y tener acceso a recursos efectivos cuando sean objeto de medidas de vigilancia.

6. Fortalecer los programas de alfabetización digital con la finalidad de combatir la desinformación o manipulación de información en línea. Asimismo, corresponde revisar los marcos normativos que regulan la publicidad en línea durante períodos electorales para garantizar, en la mayor medida posible, una protección reforzada de los derechos a la libertad de expresión y de participación política.
7. Establecer parámetros para el desarrollo de nuevas tecnologías en el ámbito de salud con un enfoque centrado en la protección de los derechos humanos. En específico, adoptar medidas para evitar eventuales violaciones de la privacidad y de la autonomía de los y las pacientes. En este sentido, la legislación nacional debe otorgar protección contra la divulgación de datos médicos sensibles.
8. Implementar políticas que aseguren la conectividad universal, y que contengan medidas positivas para cerrar las brechas de acceso de los grupos en situación de vulnerabilidad. Asimismo, deben incluir medidas para abordar las disparidades de género preexistentes y responder a las cargas de trabajo desproporcionadas sobre las mujeres.
9. Crear un marco normativo, políticas y programas que promuevan la protección social de personas trabajadoras mediante las plataformas digitales, que incluya sistemas de supervisión para garantizar la seguridad y salud en el trabajo.
10. Promover y garantizar el diálogo y la participación de la sociedad civil y las empresas tecnológicas durante los ciclos de las políticas públicas vinculadas con el uso de las nuevas tecnologías.
11. Prestar especial atención a la protección de los derechos en línea de grupos en situación de vulnerabilidad, como NNA, personas mayores, mujeres y minorías. De igual forma, deben promover medidas para prevenir el acoso y la discriminación en línea.
12. Colaborar a nivel internacional para abordar los desafíos transfronterizos relacionados con las nuevas tecnologías. Esto incluye la cooperación en la lucha contra la ciberdelincuencia y la promoción de estándares de derechos humanos en foros internacionales.
13. Implementar programas de fortalecimiento de capacidades de forma continua para operadores de justicia y fuerzas de seguridad con el objetivo de dotarlos de las habilidades y los conocimientos necesarios para abordar los desafíos emergentes relacionados con las nuevas tecnologías y la protección de derechos en el entorno digital.
14. Promover el diálogo con las organizaciones de la sociedad civil, expertos en tecnología, la academia y defensores de derechos humanos en el desarrollo de políticas y regulaciones relacionadas con las nuevas tecnologías.

Estas recomendaciones son fundamentales y no exclusivas para asegurar que los Estados, protejan los derechos humanos en la era digital y aborden los desafíos planteados por las nuevas tecnologías de manera efectiva y respetuosa de los derechos de las personas.

8. REFERENCIAS

- ACNUDH. (2017). Promoción, protección y disfrute de los derechos humanos en Internet: medios de cerrar la brecha digital entre los géneros desde una perspectiva de derechos humanos, A/HRC/35/9.
- (2018). El derecho a la privacidad en la era digital, A/HRC/39/29.
 - (2020). Impacto de las nuevas tecnologías en la promoción y protección de los derechos humanos en el contexto de las reuniones, incluidas las protestas pacíficas, A/HRC/44/24.
 - (2021). El derecho a la privacidad en la era digital, A/HRC/48/31.
 - (2022, 16 de septiembre). Instrumentos de espionaje y vigilancia: aumentan las amenazas a la intimidad y los derechos humanos, advierte un informe de las Naciones Unidas [Comunicado de prensa]. <https://www.ohchr.org/es/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing-un-report>
- Article 19. (2021, 28 de octubre). Organizaciones advierten riesgos de tecnologías de vigilancia a los derechos humanos en audiencia ante la CIDH. <https://articulo19.org/organizaciones-advierten-riesgos-de-tecnologias-de-vigilancia-a-los-derechos-humanos-en-audiencia-ante-la-cidh/>
- Asamblea General de las Naciones Unidas. (2015). El derecho a la privacidad en la era digital, A/RES/69/166.
- (2018). Las tecnologías de la información y las comunicaciones para el desarrollo sostenible, A/RES/72/200.
- Asquerino, M. (2022). Algoritmos y discriminación. En J. M. Morales (Ed.). Realidad social y discriminación: estudios sobre diversidad e inclusión laboral (pp. 335-382). Universidad de Sevilla. <https://idus.us.es/bitstream/handle/11441/142652/Algoritmos%20y%20discriminacion.pdf?sequence=1&isAllowed=y>
- Banco Interamericano de Desarrollo (BID). (2021). Posibles transformaciones en salud, educación y trabajo a través de la digitalización en la salida de la pandemia en América Latina y el Caribe. <https://publications.iadb.org/es/posibles-transformaciones-en-salud-educacion-y-trabajo-traves-de-la-digitalizacion-en-la-salida-de>
- BBC Mundo. (2017, 21 de julio). Marshall McLuhan, el «profeta de la era digital» que predijo internet 20 años antes de que se inventara. BBC News Mundo. <https://www.bbc.com/mundo/noticias-40681655>
- Britts Imperial University. (2023, 14 de abril). The Relationship Between Big Data and Artificial Intelligence. LinkedIn. <https://www.linkedin.com/pulse/relationship-between-big-data-artificial-intelligence/>
- Castells, M. (2009). Comunicación y poder. Alianza Editorial.
- CEPAL. (2021a). Tecnologías digitales para un nuevo futuro. https://repositorio.cepal.org/bitstream/handle/11362/46816/1/S2000961_es.pdf
- (2021b). La autonomía económica de las mujeres en la recuperación sostenible y con igualdad. Informe Especial COVID-19 N.º 9. <https://www.cepal.org/es/publicaciones/46633-la-autonomia-economica-mujeres-la-recuperacion-sostenible-igualdad>
 - (2021c). Coyuntura laboral en América Latina y el Caribe: trabajo decente para los trabajadores de plataformas en América Latina. <https://www.cepal.org/es/publicaciones/46955-coyuntura-laboral-america-latina-caribe-trabajo-decente-trabajadores-plataformas>

- CIDH. (2018, 2 de mayo). Declaración Conjunta sobre la Independencia y la Diversidad de los Medios de Comunicación en la era digital. <https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=1101&IID=2>
- (2019, 4 de mayo). Informe N.º 57/19 (Informe de fondo). Caso Miembros de la Corporación Colectiva de Abogados José Alvear Restrepo c. Colombia. https://www.oas.org/es/cidh/decisiones/corte/2020/CO_12.380_ES.PDF
 - (2020). Declaración Conjunta sobre Libertad de Expresión y Elecciones en la era digital. <https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=1174&IID=2>
 - (2021a, 1 de octubre). La CIDH y su RELE llaman a los Estados a adoptar medidas para reducir las brechas digitales de las personas mayores [Comunicado de prensa]. <https://www.oas.org/pt/CIDH/jsForm/?File=/es/cidh/prensa/comunicados/2021/259.asp>
 - (2021b, 6 de agosto). La CIDH, su RELE y ONU-DH México manifiestan preocupación ante nuevos hallazgos sobre la utilización del *software* Pegasus [Comunicado de prensa]. <https://www.oas.org/es/cidh/expresion/showarticle.asp?IID=2&artID=1207>
 - (2021c, 27 de octubre). Uso de tecnologías de vigilancia y su impacto en la libertad de expresión en pandemia [Video]. YouTube. https://www.youtube.com/watch?v=IdkYQIp-BhoE&ab_channel=Comisi%C3%B3nInteramericanadeDerechosHumanos
 - (2022a). Informe Anual de la Comisión Interamericana de Derechos Humanos 2021. <https://www.oas.org/es/cidh/expresion/informes/IA2021ESP.pdf>
 - (2022b, 31 de enero). La CIDH, RELE y OACNUDH expresan preocupación ante los hallazgos sobre uso del *software* Pegasus para espiar a periodistas y organizaciones de la sociedad civil en El Salvador [Comunicado de prensa]. <https://www.oas.org/es/CIDH/jsForm/?File=/es/cidh/prensa/comunicados/2022/022.asp>
 - (2023a, 2 de junio). CIDH manifiesta su preocupación por el aumento de casos sobre el uso de pegasus en México [Comunicado de prensa]. <https://www.oas.org/es/CIDH/jsForm/?File=/es/cidh/prensa/comunicados/2023/109.asp>
 - (2023b, 31 de marzo). La RELE visitó empresas y organizaciones de Internet, para dialogar sobre prácticas en derechos humanos y tecnología [Comunicado de prensa]. <https://www.oas.org/es/cidh/expresion/showarticle.asp?IID=2&artID=1271>
- Columbia Engineering. (s/f). Artificial Intelligence (AI) vs. Machine Learning. <https://ai.engineering.columbia.edu/ai-vs-machine-learning/>
- Comité Asesor del Consejo de Derechos Humanos. (2021). Impactos, oportunidades y retos que pueden entrañar las tecnologías digitales nuevas y emergentes en relación con la promoción y la protección de los derechos humanos, A/HRC/47/52.
- Comité de Derechos Humanos. (1998). Observación General n.º 16 relativa al derecho a la intimidad, HRI/GEN/1/Rev.9 (Vol. I).
- (2011). Observación General n.º 34 relativa a la libertad de opinión y de expresión, CCPR/C/GC/34.
- Comité DESC. (1983). Observación General n.º 10. El derecho a la libertad de opinión (art. 19). En Recopilación de las observaciones y recomendaciones generales adoptadas por órganos creados en virtud de tratados de derechos humanos, HRI/GEN/1/Rev.9 (Vol.I)
- (1999). Observación General n.º 13. El derecho a la educación (artículo 13 del Pacto), E/C.12/1999/10.
 - (2000). Observación General n.º 14. El derecho al disfrute del más alto nivel posible de salud, E/C.12/2000/4.
 - (2006). Observación General n.º 18. El derecho al trabajo, E/C.12/GC/18.
 - (2020). Observación General n.º 25, relativa a la ciencia y los derechos económicos, sociales y culturales (artículo 15, párrafos 1 b), 2, 3 y 4, del Pacto Internacional de Derechos Económicos, Sociales y Culturales), E/C.12/GC/25.
- Comité de los Derechos del Niño. (2021). Observación General n.º 25 relativa a los derechos de los niños en relación con el entorno digital, CRC/C/GC/25.

- Comité Jurídico Interamericano. (2023). Declaración sobre Neurociencia, Neurotecnologías y Derechos Humanos: Nuevos Desafíos Jurídicos para las Américas. CJI/RES. 281 (CII-O/23) corr.1. https://www.oas.org/es/sla/cji/docs/CJI-RES_281_CII-O-23_corr1_ESP.pdf
- Comité para la Eliminación de la Discriminación Racial. (2013). Recomendación General n.º 35 relativa a la lucha contra el discurso de odio racista, CERD/C/GC/35.
- Consejo de Europa. (2003). Defamation and Freedom of Expression. <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680483b2d>
- (2017a). Filtering, blocking and take-down of illegal content on the Internet. <https://edoc.coe.int/en/Internet/7289-pdf-comparative-study-on-blocking-filtering-and-take-down-of-illegal-Internet-content.html>
 - (2017b). Report by the Committee of experts on cross-border flow of Internet traffic and Internet freedom on Freedom of assembly and association on the Internet. <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168064ac99>
 - (2019). Freedom of expression in 2018. <https://edoc.coe.int/en/fundamental-freedoms/7912-freedom-of-expression-in-2018.html#>
 - (2020). Prioritisation uncovered: The Discoverability of Public Interest Content Online. <https://rm.coe.int/publication-content-prioritisation-report/1680a07a57>
 - (2021). Content Moderation: Best practices towards effective legal and procedural frameworks for self-regulatory and co-regulatory mechanisms of content moderation. Nota de orientación adoptada por el Comité Directivo de Medios y Sociedad de la Información. <https://rm.coe.int/content-moderation-en/1680a2cc18>
 - (2022). Freedom of expression in 2021. Informe del Departamento de la Sociedad de la Información, DGI(2022) 2. <https://rm.coe.int/freedom-of-expression-2021-en/1680a6525e>
- Corte Constitucional de Colombia. (2012a). Sentencia T-260/12. <https://www.corteconstitucional.gov.co/relatoria/2012/t-260-12.htm>
- (2012b). Sentencia 458/12. https://www.funcionpublica.gov.co/eva/gestornormativo/norma_pdf.php?i=49067
 - (2013). Sentencia de Tutela 453/13. https://www.icbf.gov.co/cargues/avance/docs/t-453_1913.htm
- Corte IDH. (1985). Opinión Consultiva OC-5/85 del 13 de noviembre de 1895. La colegiación obligatoria de periodistas (artículos. 13 y 29 de la Convención Americana sobre Derechos Humanos). https://www.corteidh.or.cr/docs/opiniones/seriea_05_esp.pdf
- (2004). Sentencia del caso Herrera Ulloa vs. Costa Rica (Excepciones preliminares, Fondo, Reparaciones y Costas). https://www.corteidh.or.cr/docs/casos/articulos/seriec_107_esp.pdf
 - (2008). Sentencia del caso Castañeda Gutman vs. Estados Unidos Mexicanos (Excepciones preliminares, Fondo, Reparaciones y Costas). https://www.corteidh.or.cr/docs/casos/articulos/seriec_184_esp.doc
 - (2009a). Sentencia del caso Perozo y otros vs. Venezuela (Excepciones preliminares, Fondo, Reparaciones y Costas).
 - (2009b). Sentencia del caso Ríos y otros vs. Venezuela (Excepciones preliminares, Fondo, Reparaciones y Costas)
 - (2009c). Sentencia del caso Escher y otros vs. Brasil (Excepciones preliminares, Fondo, Reparaciones y Costas).
 - (2012). Sentencia del caso Artavia Murillo vs. Costa Rica (Excepciones preliminares, Fondo, Reparaciones y Costas). https://www.corteidh.or.cr/docs/casos/articulos/seriec_257_esp.pdf

- (2015). Sentencia del caso Gonzales Lluy y otros vs. Ecuador (Excepciones preliminares, Fondo, Reparaciones y Costas).
- (2017). Sentencia del caso Lagos del Campo vs. Perú (Excepciones preliminares, Fondo, Reparaciones y Costas).
- (2020). Sentencia del caso Spoltore vs. Argentina (Excepción Preliminar, Fondo, Reparaciones y Costas).
- (2021a). Opinión Consultiva OC-27/21 (Derechos a la libertad sindical, negociación colectiva y huelga, y su relación con otros derechos, con perspectiva de género).
- (2021b). Sentencia del caso Buzos Miskitos (Lemoth Morris y otros) vs. Honduras.
- (2021c). Sentencia del caso Casa Nina vs. Perú (Excepciones preliminares, Fondo, Reparaciones y Costas).
- (2021d). Sentencia del caso Extrabajadores del Organismo Judicial vs. Guatemala (Excepciones Preliminares, Fondo y Reparaciones).
- (2021e). Sentencia del caso Manuela y otros vs. El Salvador (Excepciones preliminares, Fondo, Reparaciones y Costas).
- (2022a). Sentencia del caso Brítez Arce y otros vs. Argentina (Fondo, Reparaciones y Costas).
- (2022b). Sentencia del caso Nissen Pessolani vs. Paraguay (Fondo, Reparaciones y Costas).
- (2023). Sentencia del caso Aguinaga Aillón vs. Ecuador (Fondo, Reparaciones y Costas).

Corte Suprema de Chile. (2023). GIRARDI/EMOTIV INC (Rol: 105065-2023). <https://img.lpderecho.pe/wp-content/uploads/2023/08/sentencia-217225-2023-LPDerecho.pdf>

Corte Suprema de Justicia de la Nación. (2014). Rodríguez, María Belén c/ Google Inc. y otros/ daños y perjuicios. <http://www.saij.gov.ar/corte-suprema-justicia-nacion-federal-ciudad-autonoma-buenos-aires-rodriguez-maria-belen-google-inc-otro-danos-perjuicios-fa14000161-2014-10-28/123456789-161-0004-lots-eupmocsollaf>

Dalla, A. (2011). Los derechos políticos en el Sistema Interamericano de Derechos Humanos. <https://www.corteidh.or.cr/tablas/r30080.pdf>

Derechos Digitales. (2020a). 2010-2020. Sucesos regulatorios en materia de privacidad e Internet en Latinoamérica. <https://www.derechosdigitales.org/wp-content/uploads/tendencias-privacidad-latam.pdf>

- (2020b). Narrativas en torno al uso de la huella digital en la salud pública. <https://www.derechosdigitales.org/wp-content/uploads/huelladigital-saludpublica-1.pdf>

Del Sesto R. y Kwon, T. (2023). The United States' approach to AI regulation: Key Considerations for companies. Morgan Lewis. <https://www.morganlewis.com/pubs/2023/05/the-united-states-approach-to-ai-regulation-key-considerations-for-companies>

Dhaliwal, M. (2020, 6 de febrero). Las promesas y los peligros de la salud digital. Programa de Naciones Unidas para el Desarrollo. <https://www.undp.org/es/blog/las-promesas-y-los-peligros-de-la-salud-digital>

Díaz, M. (2018). El cuerpo como dato. Derechos Digitales.

Díaz, J. C. y Castro, A. (2021). Los derechos fundamentales y las nuevas tecnologías de la información y comunicación: una aproximación. Themis. Revista de Derecho, (79), 15-35. <https://revistas.pucp.edu.pe/index.php/themis/article/view/24862>

Dirección Regional de Protección de Datos Personales del Perú. (2015). Resolución Directoral 030-2015-JUS/DGPDP. <https://cdn.www.gob.pe/uploads/document/file/582275/RD-035-2015-DGPDP.pdf>

- El Mundo. (2017, 17 de febrero). Alemania prohíbe la muñeca Cayla por sus capacidades para el espionaje. <https://www.elmundo.es/internacional/2017/02/17/58a6e556468aeb2d-1d8b4587.html>
- Experta Independiente sobre el disfrute de todos los derechos humanos por las personas de edad de las Naciones Unidas. (2017). Los robots y los derechos: los efectos de la automatización en los derechos humanos de las personas de edad, A/HRC/36/48.
- Food and Agriculture Organization of the United Nations. (s/f). Information and Communication Technologies (ICT). <https://aims.fao.org/es/information-and-communication-technologies-ict>
- Fuentes, R. (2021, 7 de enero). El estado de la neurotecnología. Facultad de Medicina de la Universidad de Chile. <https://medicina.uchile.cl/noticias/172289/el-estado-de-la-neurotecnologia>
- García, D. (s/f). El derecho a la privacidad en las redes sociales en Internet. <https://www.cor-teidh.or.cr/tablas/r28618.pdf>
- GCF Global. (s/f). ¿Qué es *hardware* y *software*? <https://edu.gcfglobal.org/es/informatica-basica/que-es-hardware-y-software/1/>
- Gil, P. (2020, 9 de abril). Internet vs. Web: What's the Difference? Lifewire: Tech for humans. <https://www.lifewire.com/difference-between-the-internet-and-the-web-2483335>
- Gloniak, J. (1995). An Introduction to the Internet, Part 1: History, Organization and Function. Journal of Nuclear Medicine Technology. <https://tech.snmjournals.org/content/jnmt/23/2/56.full.pdf>
- Gómez, D. A., Alvarado, R. A., Martínez, M. y Díaz de León, C. (2018). La brecha digital: una revisión conceptual y aportaciones metodológicas para su estudio de México. *Entreciencias: Diálogos en la Sociedad del Conocimiento*, 6(16). <https://doi.org/10.22201/enesl.20078064e.2018.16.62611>
- González, J. (2019). El derecho al olvido en España y en la UE. *Dialnet*, 13(2), 57-63. <https://dialnet.unirioja.es/servlet/articulo?codigo=7112014>
- Hadgis, K. et al (2022, 14 de septiembre). Data Privacy: Evolving Updates to the Global Landscape. Morgan Lewis. <https://www.morganlewis.com/pubs/2022/09/data-privacy-evolving-updates-to-the-global-landscape>
- Hardy, T. IA: Inteligencia artificial. *Polis. Revista de la Universidad Bolivariana*, 1(2). <https://www.redalyc.org/pdf/305/30500219.pdf>
- Holtgrewe, U. (2014). New Technologies: The Future and the Present of Work in Information and Communication Technology. *New Technology, Work and Employment*, (29), 9-24. https://www.etui.org/sites/default/files/ez_import/holtgrewe14-newnewtech.pdf
- Hutt, R. (2018, 7 de junio). ¿Son seguros los robots «amigos» para niños? *Apolitical*. <https://apolitical.co/solution-articles/es/son-los-amigos-robot-para-ninos-seguros-alemania-no-lo-cree-asi>
- Ibáñez, M., Arroyo, L. y Collado, C. (2020). Mujeres y digitalización. De las brechas a los algoritmos. Instituto de la Mujer y para la Igualdad de Oportunidades; Ministerio de Igualdad. https://www.inmujeres.gob.es/disenovovedades/M_MUJERES_Y_DIGITALIZACION_DE_LAS_BRECHAS_A_LOS_ALGORITMOS_04.pdf

- Indecopi. (2016). Resolución Final 1050-2016/CC2. <https://servicio.indecopi.gob.pe/buscadorResoluciones/getDoc?docID=workspace://SpacesStore/ae260fca-1d32-443f-87a7-3a9ec7ca6ba6>
- Instituto Panamericano de Derecho y Tecnología. (2018, 1 de marzo). Audiencia CIDH: Inteligencia Digital, Ciberseguridad y Libertad de Expresión en América. <https://www.ipandetec.org/2018/03/01/inteligencia-digital-ciberseguridad-y-libertad-de-expresion-en-america/>
- Katz, R. (2015). El ecosistema y la economía digital en América Latina. Ariel; Fundación Telefónica; Planeta.
- Koridor Inc. (2022, 20 de abril). What's the Difference Between AI and Algorithm? LinkedIn. <https://www.linkedin.com/pulse/whats-difference-between-ai-algorithm-koridorapp/>
- Landa, C. (2023). Revolución digital y Constitución. Palestra Editores.
- Lara, D. (2015). Grupos en situación de vulnerabilidad. Comisión Nacional de Derechos Humanos de México. https://appweb.cndh.org.mx/biblioteca/archivos/pdfs/fas_CTDH_GruposVulnerabilidadlaReimpr.pdf
- Molestina, M. (2008). Internet y la promoción de los derechos humanos. Revista IIDH, (47), 183-202. <https://www.corteidh.or.cr/tablas/r23828.pdf>
- Noticias ONU. (2023, 6 de julio). La inteligencia artificial precisa de una regulación para que beneficie a todos. <https://news.un.org/es/story/2023/07/1522542>
- OCDE. (2022). Declaration on Government Access to Personal Data Held by Private Sector Entities. <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487>
- (2023). Líneas Directrices de la OCDE para Empresas Multinacionales sobre Conducta Empresarial Responsable. https://www.oecd-ilibrary.org/finance-and-investment/lineas-directrices-de-la-ocde-para-empresas-multinacionales-sobre-conducta-empresarial-responsable_7abea681-es
- OEA. (2021, 1 de octubre). La CIDH y su RELE llaman a los Estados a adoptar medidas para reducir las brechas digitales de las personas mayores [Comunicado de prensa]. <https://www.oas.org/pt/CIDH/jsForm/?File=/es/cidh/prensa/comunicados/2021/259.asp>
- (2022). Principios actualizados sobre la privacidad y la protección de datos personales. https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf
- OIT. (2021). Perspectivas sociales y del empleo en el mundo. Resumen Ejecutivo. https://www.ilo.org/wcmsp5/groups/public/---dgreports/---dcomm/documents/publication/wcms_771675.pdf
- (2022a, 9 de septiembre). La OIT destaca el potencial de las tecnologías para impulsar la e-formalización en América Latina. https://www.ilo.org/americas/sala-de-prensa/WCMS_855184/lang--es/index.htm
- (2022b). E-formalización en América Latina: acelerando en una región llena de brechas. https://www.ilo.org/wcmsp5/groups/public/---americas/---ro-lima/documents/publication/wcms_854208.pdf
- (s/f). New technologies are bringing opportunities and challenges to working lives. https://www.ilo.org/global/topics/future-of-work/trends/WCMS_545675/lang--en/index.htm
- ONU. (s/f a). Relator Especial sobre el Derecho a la Privacidad. Finalidad del mandato. <https://www.ohchr.org/es/special-procedures/sr-privacy>

- (s/f b). Derecho Internacional de los Derechos Humanos. <https://www.ohchr.org/es/instruments-and-mechanisms/international-human-rights-law>
 - (2022, 15 de junio). UN experts highlight digital rights in conflict and humanitarian crises at RightsCon [Comunicado de prensa]. <https://www.ohchr.org/en/press-releases/2022/06/un-experts-highlight-digital-rights-conflict-and-humanitarian-crises>
 - (2023, 2 de junio). Las tecnologías nuevas y emergentes necesitan una supervisión urgente y una transparencia sólida: expertos de la ONU [Comunicado de prensa]. <https://www.ohchr.org/en/press-releases/2022/06/un-experts-highlight-digital-rights-conflict-and-humanitarian-crises>
- Orenga, J. (2022). Impactos del uso de las nuevas tecnologías digitales en la libertad de expresión. Institut de Drets Humans de Catalunya. <https://www.idhc.org/arxius/recerca/1653294056-Tecnologias-digitales-libertad-expresion.pdf>
- Orias, R. (2022). Los neuro derechos. Una nueva frontera para los derechos humanos. *Agenda Internacional*, (40), 211-227.
- Panel de Alto Nivel sobre la Cooperación Digital. (2019). La era de la interdependencia digital. Informe del Panel de Alto Nivel del Secretario General sobre la Cooperación Digital. <https://www.un.org/sites/www.un.org/files/uploads/files/es/HLP%20on%20Digital%20Cooperation%20Report%20Executive%20Summary%20-%20ES%20.pdf>
- Parlamento Europeo. (2023a, 14 de junio). MEPs ready to negotiate first-ever rules for safe and transparent AI. Noticias: Parlamento Europeo. <https://www.europarl.europa.eu/news/en/press-room/20230609IPR96212/meps-ready-to-negotiate-first-ever-rules-for-safe-and-transparent-ai>
- (2023b, 12 de junio). Ley de IA de la UE: primera normativa sobre inteligencia artificial. Noticias: Parlamento Europeo. <https://www.europarl.europa.eu/news/es/headlines/society/20230601STO93804/ley-de-ia-de-la-ue-primer-normativa-sobre-inteligencia-artificial>
- Pérez, J. y Núñez, J. (2017). Regulación del ecosistema digital. Universidad Externado de Colombia.
- Privacy International. (2013). Biometrics: friend or foe of privacy. <https://privacyinternational.org/news-analysis/1409/biometrics-friend-or-foe-privacy>
- Rajan, A. (2018, 18 de enero). 8 razones que muestran que Facebook alcanzó su punto máximo y ahora puede estar perdiendo influencia. BBC News Mundo. <https://www.bbc.com/mundo/noticias-43106226>
- Relator Especial de las Naciones Unidas sobre la Promoción y Protección del Derecho a la Libertad de Opinión y de Expresión, Representante para la Libertad de los Medios de Comunicación de la Organización para la Seguridad y Cooperación en Europa (OSCE), Relator Especial para la Libertad de Expresión de la Organización de los Estados Americanos (OEA) y Relator Especial sobre Libertad de Expresión y Acceso a la Información de la Comisión Africana sobre Derechos Humanos y de los Pueblos (CADHP). (2018). Declaración Conjunta sobre la Independencia y la Diversidad de los Medios de Comunicación en la era digital. <https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=1100&IID=2>
- Relator Especial para la Libertad de Expresión de la CIDH. (2013). Libertad de expresión e Internet.
- Relatora Especial sobre el derecho a la educación de la ONU. (2022). Repercusiones de la digitalización de la educación en el derecho a la educación, A/HRC/50/32.

- Relatora Especial sobre el derecho a la privacidad de la ONU. (2022a). La privacidad y la protección de datos personales en Iberoamérica: ¿un paso hacia la globalización?, A/HRC/49/55.
- (2022b). Principios que informan la privacidad y la protección de datos personales, A/77/196.
- Relator Especial sobre la Libertad de Reunión Pacífica y de Asociación de la ONU. (2021). Informe del Relator Especial sobre la Libertad de Reunión Pacífica y de Asociación de la ONU, Clément N. Voule. Poner fin a los apagones de Internet: un camino a seguir, A/HRC/47/24/Add.2.
- Relator Especial sobre la Promoción y Protección del Derecho a la Libertad de Opinión y de Expresión de la ONU. (1998). Promoción y protección del derecho a la libertad de opinión y de expresión. Informe del Relator Especial, Sr. Abid Hussain, presentado en cumplimiento de la resolución 1997/27 de la Comisión de Derechos Humanos, E/CN.4/1998/40.
- (2010). Declaración Conjunta del Décimo Aniversario: Los diez principales desafíos a la libre expresión en la próxima década, A/HRC/14/23/Add.2. 25 de marzo de 2010.
 - (2012). Informe del Relator especial sobre la Promoción y Protección del Derecho a la Libertad de Opinión y Expresión, Frank La Rue, A/HRC/20/17. 4 de junio de 2012.
 - (2014). Informe presentado durante el 26° periodo de sesiones del Consejo de Derechos Humanos, A/HRC/26/30.
 - (2021). Informe de la Relatora Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Irene Khan. La desinformación y la libertad de opinión y de expresión, A/HRC/47/25.
- Relatora Especial sobre las formas contemporáneas de racismo, discriminación racial, xenofobia y formas conexas de intolerancia de la ONU. (2020a). La discriminación racial y las tecnologías digitales emergentes: un análisis de los derechos humanos, A/HRC/44/57.
- (2020b). Informe de la Relatora Especial sobre las formas contemporáneas de racismo, discriminación racial, xenofobia y formas conexas de intolerancia, E. Tendayi Achiume, A/75/590.
- Relatoría Especial para la Libertad de Expresión de la CIDH. (2017). Estándares para una Internet Libre, Abierta e Incluyente. OEA/Ser.L/V/II. CIDH/RELE/INF.17/17. http://www.oas.org/es/cidh/expresion/docs/publicaciones/internet_2016_esp.pdf
- (2019a). Niñez, libertad de expresión y medios de comunicación, CIDH/RELE/INF.23/19. <https://www.oas.org/es/cidh/expresion/informes/Nin%CC%83ezLEXMediosESP.pdf>
 - (2019b). Protesta y Derechos Humanos: Estándares sobre los derechos involucrados en la protesta social y las obligaciones que deben guiar la respuesta estatal, CIDH/RELE/INF.22/19. <https://www.oas.org/es/cidh/expresion/publicaciones/ProtestayDerechosHumanos.pdf>
 - (2020, 31 de agosto). Estados de la región deben acelerar políticas de acceso universal a Internet durante la pandemia del COVID-19 y adoptar medidas diferenciadas para incorporar a grupos en situación de vulnerabilidad, R206/20 [Comunicado de prensa]. <https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=1182&lID=2>
- Relatoría Especial sobre la violencia contra la mujer, sus causas y consecuencias. (2018). Informe de la Relatora Especial sobre la violencia contra la mujer, sus causas y consecuencias relativo a su misión a Australia, A/HRC/38/47/Add.1.
- Reyes, V. (Coord.). (2023). Relatoría del conversatorio Nuevas tecnologías y derechos humanos: impactos, desafíos y oportunidades en la era de la conectividad digital. Instituto de Democracia y Derechos Humanos de la Pontificia Universidad Católica del Perú. <https://repositorio.pucp.edu.pe/index/handle/123456789/193096>
- Rodríguez-Andrés, R. (2018). Trump 2016: ¿presidente gracias a las redes sociales? <https://dialnet.unirioja.es/servlet/articulo?codigo=6496368>

- Royde-Smith, J. (s/f). Costs of the war Killed, wounded, prisoners, or missing. Britannica. <https://www.britannica.com/event/World-War-II/Human-and-material-cost>
- Ruiz, M., Rodríguez, J. y Olivares, J. (2009). Una mirada a la biometría. *Revista Avances en Sistemas e Informática*, 6(2), 29-38. <https://www.redalyc.org/pdf/1331/133113598005.pdf>
- Sáenz, P. y Botero, C. (2015). En Colombia, el puma no es como lo pintan. *Digital Rights*. <https://digitalrightslac.derechosdigitales.org/es/en-colombia-el-puma-no-es-como-lo-pintan/>
- Sáinz, M., Arroyo, L. y Castaño, C. (2020). Mujeres y digitalización. De las brechas a los algoritmos. Instituto de la Mujer y para la Igualdad de Oportunidades.
- Sales, P. (2021). Algorithms, Artificial Intelligence, and the Law. Duke University School of Law. https://judicature.duke.edu/wp-content/uploads/2021/04/Sales_Spring2021.pdf
- Salmón, E. (2019). Curso de Derecho Internacional Público. Fondo Editorial PUCP.
- Sarker, I. (2021). Machine Learning: Algorithms, Real-World Applications and Research Directions. *SN Computer Science*. <https://doi.org/10.1007/s42979-021-00592-x>
- Schwab, K. (2016). The Fourth Industrial Revolution. World Economic Forum.
- Secretario General de las Naciones Unidas. (2018). Estrategia del Secretario General de Naciones Unidas en materia de nuevas tecnologías. <https://www.un.org/en/newtechnologies/imLages/pdf/SGs-Strategy-on-New-Technologies-ES.pdf>
- (2020a). Cuestión del ejercicio efectivo, en todos los países, de los derechos económicos, sociales y culturales: la función de las nuevas tecnologías en el ejercicio efectivo de los derechos económicos, sociales y culturales, A/HRC/43/29.
 - (2020b). Hoja de ruta para la cooperación digital: aplicación de las recomendaciones del Panel de Alto Nivel sobre la Cooperación Digital, A/74/821.
- Tang, K. y Spijkers, O. (2022). The Human Right to a Clean, Healthy and Sustainable Environment. *Chinese Journal of Environmental Law*, 6(1), 87-107. <https://doi.org/10.1163/24686042-12340078>
- Tapiador M. (2005). Tecnologías biométricas aplicadas a la seguridad. Rama.
- TEDH. (2013). Caso of Nagla v. Latvia. Demanda 73469/10. <https://hudoc.echr.coe.int/fre#%7B%22fulltext%22:%5B%22Case%20of%20Nagla%20v.%20Latvia.%22%5D,%22itemid%22:%5B%22002-7640%22%5D%7D>
- (2017). Caso Bărbulescu Contra Romania. Demanda 61496/08. <https://www.mjusticia.gob.es/es/AreaInternacional/TribunalEuropeo/Documents/Sentencia%20Barbulescu%20c.%20Ruman%C3%ADa.pdf>
 - (2021). Caso Big Brother Watch y otros v. Reino Unido. <https://hudoc.echr.coe.int/fre#%7B%22itemid%22:%5B%22001-210077%22%7D>
- Téllez, E. (2020). Análisis documental sobre el tema del Big Data y su impacto en los derechos humanos. *Derecho PUCP*, (84), 157-158. <https://dx.doi.org/10.18800/derechopucp.202001.006>
- Tribunal Constitucional del Perú. (2028). Sentencia del caso de la in QUO regula el gasto de publicidad estatal. <https://tc.gob.pe/jurisprudencia/2018/00012-2018-AI.pdf>
- UNESCO (2001). The new information and communication technologies for the development of education, science and culture. <https://unesdoc.unesco.org/ark:/48223/pf0000122593>

- (2021a). El aporte de la inteligencia artificial y las TIC avanzadas a las sociedades del conocimiento: una perspectiva de derechos, apertura, acceso y múltiples actores. <https://unesdoc.unesco.org/ark:/48223/pf0000375796>
- (2021b). *Recomendación sobre la Ética de la Inteligencia Artificial*. https://unesdoc.unesco.org/ark:/48223/pf0000380455_spa
- (2023). Unveiling the neurotechnology landscape: scientific advancements innovations and major trends. <https://unesdoc.unesco.org/ark:/48223/pf0000386137>

United States Holocaust Memorial Museum. (2020, 8 de diciembre). Documenting numbers of victims of the holocaust and nazi persecution. Holocaust Encyclopedia. <https://encyclopedia.ushmm.org/content/en/article/documenting-numbers-of-victims-of-the-holocaust-and-nazi-persecution>

Ureña, R. (2019). Autoridad algorítmica: ¿cómo empezar a pensar la protección de los derechos humanos en la era del «big data»? *Latin American Law Review*, (2). <https://doi.org/10.29263/lar02.2019.05>

UNICEF. (s/f). Informes sobre la situación de la educación durante COVID-19. La respuesta educativa de UNICEF y los gobiernos en América Latina y el Caribe. <https://www.unicef.org/lac/respuesta-educativa-de-alc-frente-al-covid-19>

- (2020). LACRO COVID 19 Respuesta Educativa: Alcanzando a los niños más vulnerables. <https://www.unicef.org/lac/en/media/14531/file>

UNICEF y UNESCO. (2023). Políticas digitales en educación en América Latina. Tendencias emergentes en contexto de pandemia y perspectivas de futuro. <https://www.unicef.org/lac/informes/politicas-digitales-educacion-america-latina-tendencias-emergentes>

Unión Europea. (2000). Carta de Derechos Fundamentales https://www.right-to-education.org/sites/right-to-education.org/files/resource-attachments/EU_Carta_Derechos_Fundamentales_Uni%C3%B3n_Europea_2000_ES.pdf

Velasco, P. y Venturini, J. (2021). Decisiones automatizadas en la función pública en América Latina. Una aproximación comparada a su aplicación en Brasil, Chile, Colombia y Uruguay. *Derechos Digitales*. https://www.derechosdigitales.org/wp-content/uploads/CPC_informeComparado.pdf

Walter de Santana, A. y Archegas, J. (2022a, 19 de agosto). Populismo digital en Brasil: las respuestas estatales y privadas, Introducción. *Agenda Estado de Derecho*. <https://agendaestadodederecho.com/populismo-digital-en-brasil-las-respuestas-estatales-y-privadas-parte-1/>

- (2022b, 19 de agosto). Populismo digital en Brasil: las respuestas estatales y privadas, primera entrega. *Agenda Estado de Derecho*. <https://agendaestadodederecho.com/populismo-digital-en-brasil-las-respuestas-estatales-y-privadas-parte-2/>

Woodward, J. D. (1997). Biometrics: Privacy's foe or Privacy's friend? *Proceedings of the IEEE*, 85(9), 1480-1492. <https://doi.org/10.1109/5.628723>

ISBN: 978-612-4474-48-4



9 786124 474484

INFORME DE INVESTIGACIÓN NUEVAS TECNOLOGÍAS Y DERECHOS HUMANOS: IMPACTOS, DESAFÍOS Y OPORTUNIDADES EN LA ERA DE LA CONECTIVIDAD DIGITAL



IDEHPUCP



ESTADO DE DERECHO · LATINOAMÉRICA