



Asamblea General

Distr. general
29 de agosto de 2025
Español
Original: inglés

Consejo de Derechos Humanos

60º período de sesiones

8 de septiembre a 3 de octubre de 2025

Temas 2 y 3 de la agenda

**Informe anual del Alto Comisionado de las Naciones Unidas
para los Derechos Humanos e informes de la Oficina del
Alto Comisionado y del Secretario General**

**Promoción y protección de todos los derechos humanos,
civiles, políticos, económicos, sociales y culturales,
incluido el derecho al desarrollo**

El derecho a la privacidad en la era digital

Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos*

Resumen

Este informe, presentado en cumplimiento de la resolución 54/21 del Consejo de Derechos Humanos, contiene un análisis de los retos y riesgos en relación con la discriminación y el disfrute desigual del derecho a la privacidad asociados a la recopilación y el tratamiento de datos. Ofrece un esbozo del marco normativo aplicable, una visión de las repercusiones discriminatorias y desiguales de las tecnologías basadas en datos en sectores clave y un análisis de los factores que contribuyen a ello y de los retos resultantes. También contiene recomendaciones sobre cómo evitar que la digitalización perpetúe o profundice la discriminación y la exclusión.

* Este informe se envió a los servicios de conferencias fuera de plazo a fin de incluir la información más reciente.



I. Introducción

1. Este informe se presenta en cumplimiento de la resolución 54/21 del Consejo de Derechos Humanos, en la que el Consejo solicitó a la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (ACNUDH) que preparase un informe sobre los retos y riesgos en relación con la discriminación y el disfrute desigual del derecho a la privacidad asociados a la recopilación y el tratamiento de datos, que sirviera para determinar y aclarar los principios de derechos humanos, las salvaguardias y las mejores prácticas conexas, y que presentase el informe al Consejo en su 57º período de sesiones. Debido a la actual crisis de liquidez que afecta a la Secretaría, la presentación del informe se aplazó hasta el 60º período de sesiones.

2. La transformación digital de las sociedades es un avance definitorio de los tiempos actuales, que opera cambios en las economías, los entornos políticos y la cultura. Se basa en la recopilación y el tratamiento de datos a una escala sin precedentes. Internet, en particular, aparece como una fuente ilimitada de datos que pueden recopilarse, compartirse, analizarse, utilizarse y transformarse en los principales elementos constitutivos de aplicaciones en casi todos los ámbitos de la vida humana. Los avances en inteligencia artificial se han basado en esos procesos y han intensificado en mayor medida la búsqueda de más datos. Paralelamente, en las dos últimas décadas se ha hecho cada vez más evidente que los beneficios y los perjuicios de la digitalización se distribuyen de forma desigual. La discriminación y la desigualdad derivadas de la recopilación y el tratamiento de datos están muy extendidas y pueden observarse en todos los sectores de la sociedad: por ejemplo, los generadores de imágenes que solo producen imágenes de médicos de piel clara, incluso cuando se les pide expresamente que sean más inclusivos; el hecho de que las mujeres no reciban ofertas de empleo para puestos directivos; la caracterización de una persona como terrorista sobre la base de perfiles algorítmicos discriminatorios; la detención injusta de personas negras por un reconocimiento facial inexacto; el hecho de que un padre con discapacidad sea investigado erróneamente por maltrato infantil debido a un sesgo inherente a los sistemas algorítmicos de modelización de riesgos de los organismos de protección de menores; el enjuiciamiento de mujeres por haber ejercido sus derechos de salud sexual y reproductiva, basándose en datos recopilados de aplicaciones de seguimiento de sus períodos; o la incapacidad de los trabajadores agrícolas de recibir ayudas sociales porque sus huellas dactilares no pueden ser leídas por los sistemas de identificación biométrica debido a décadas de trabajo manual.

3. El presente informe ofrece una visión de estos fenómenos, sus repercusiones y los factores que contribuyen a ellos, y propone vías para superar y prevenir la discriminación y la desigualdad. Se basa en informes anteriores publicados por el Secretario General y el ACNUDH en los que se abordaban muchas de las complejas cuestiones de la digitalización y la datificación¹, y refleja las respuestas recibidas a la solicitud de contribuciones formulada por el ACNUDH².

II. Marco normativo

A. Derecho internacional de los derechos humanos

4. El derecho a la privacidad como derecho humano está reconocido en el artículo 12 de la Declaración Universal de Derechos Humanos, en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos y en otros instrumentos internacionales y regionales de derechos humanos³. El derecho a la privacidad desempeña un papel fundamental en el equilibrio de

¹ A/HRC/27/37, A/HRC/39/29, A/HRC/43/29, A/HRC/48/31, A/HRC/51/17, A/HRC/59/32 y A/79/296.

² Véase <https://www.ohchr.org/en/calls-for-input/2025/right-privacy-digital-age>.

³ Véanse el artículo 16 de la Convención sobre los Derechos del Niño, el artículo 14 de la Convención Internacional sobre la Protección de los Derechos de Todos los Trabajadores Migratorios y de Sus Familiares, el artículo 22 de la Convención sobre los Derechos de las Personas con Discapacidad, el artículo 10 de la Carta Africana sobre los Derechos y el Bienestar del Niño, el artículo 11 de la Convención Americana sobre Derechos Humanos y el artículo 8 del Convenio para la Protección de

poder entre el Estado y el individuo y es primordial para el ejercicio de los derechos en una sociedad democrática⁴. Su importancia para el goce y el ejercicio de los derechos humanos dentro y fuera de Internet⁵ en un mundo cada vez más centrado en los datos no deja de aumentar.

5. El derecho a la privacidad es vital para la dignidad humana y es un factor necesario para la protección de la autonomía y la identidad personales⁶. Protege una esfera de desarrollo autónomo, interacción y libertad, con o sin interacción con otros, libre de la intervención del Estado y de la excesiva intervención no solicitada de otros actores⁷.

6. Las dimensiones de la privacidad importantes en el contexto de la recopilación y el tratamiento de datos incluyen: la privacidad informativa, que abarca la información que existe o puede derivarse sobre una persona y su vida y las decisiones basadas en esa información⁸; la privacidad de las decisiones, que garantiza la capacidad de una persona para tomar decisiones autónomas en su vida; la privacidad corporal, que ampara el control de una persona sobre su propio cuerpo y la protege de contactos físicos, observaciones o intromisiones no deseados; y la privacidad comunicativa y asociativa, es decir, la privacidad para comunicarse y asociarse con los demás.

7. Cualquier injerencia del Estado en el derecho a la privacidad debe ser compatible con el derecho internacional de los derechos humanos y, por tanto, cumplir las normas de finalidad legítima, legalidad, necesidad y proporcionalidad⁹.

8. El derecho a la privacidad puede permitir el disfrute de otros derechos¹⁰. Así pues, la discriminación y el disfrute desigual del derecho a la privacidad en el contexto de la recopilación y el tratamiento de datos pueden afectar a otros derechos, como los derechos a la vida, la libertad y la seguridad, la libertad de expresión¹¹, la libertad de reunión pacífica¹², la libertad de circulación, el recurso efectivo, la salud, la educación y la vivienda.

9. El derecho a la igualdad y la prohibición de la discriminación son principios fundamentales del derecho internacional de los derechos humanos, afirmados en el artículo 7 de la Declaración Universal de Derechos Humanos y en los artículos 2 y 26 del Pacto Internacional de Derechos Civiles y Políticos y en otros tratados. La no discriminación es un principio intrínseco del derecho internacional, que existe no solo de forma inherente a la obligación de los Estados de garantizar el respeto, la protección y el cumplimiento de los derechos humanos sin discriminación, sino también, como se consagra en el artículo 26 del Pacto, como garantía de igualdad ante la ley y de igual protección de la ley.

10. El trato diferencial es discriminatorio si tiene por objeto o por resultado anular o menoscabar el reconocimiento, goce o ejercicio, en condiciones de igualdad, de los derechos de todas las personas, a menos que la justificación de la diferenciación sea razonable y objetiva¹³. Ello entraña evaluar si el fin y los efectos de las medidas o las omisiones de que

los Derechos Humanos y de las Libertades Fundamentales (Convenio Europeo de Derechos Humanos).

⁴ [A/HRC/39/29](#), párr. 11.

⁵ Comité de los Derechos del Niño, observación general núm. 25 (2021), relativa a los derechos de los niños en relación con el entorno digital, párrs. 67 y 68; y [A/HRC/39/29](#), párr. 11.

⁶ Comité de los Derechos del Niño, observación general núm. 25 (2021), párr. 67; y Tribunal Europeo de Derechos Humanos, *Goodwin v. the United Kingdom*, demanda núm. 28957/95, sentencia de 11 de julio de 2002, párr. 90.

⁷ Véase [A/HRC/39/29](#) y *Coeriel y Aurik c. Países Bajos* (CCPR/C/52/D/453/1991).

⁸ [A/HRC/39/29](#), párr. 5.

⁹ [A/HRC/48/31](#), párr. 8. Véase también la resolución 77/211 de la Asamblea General y la resolución 54/21 del Consejo de Derechos Humanos.

¹⁰ Véanse la resolución 54/21 del Consejo de Derechos Humanos y [A/HRC/48/31](#).

¹¹ Véase la comunicación del Centro de Estudios en Libertad de Expresión y Acceso a la Información.

¹² Véase la comunicación de Pete Fussey y Daragh Murray.

¹³ Comité de Derechos Humanos, observación general núm. 18 (1989), relativa a la no discriminación y los derechos económicos, sociales y culturales, párrs. 6 y 13; y Comité de Derechos Económicos, Sociales y Culturales, observación general núm. 20 (2009) relativa a la no discriminación y los derechos económicos, sociales y culturales, párr. 13.

se trate son legítimos, están dirigidos a promover el bienestar general en una sociedad democrática y son proporcionados¹⁴.

11. Los tratados de derechos humanos prohíben la discriminación por motivos de raza, color, sexo, idioma, religión, opinión política o de otra índole, origen nacional o social, posición económica, nacimiento u otros factores. La referencia a “otros factores” en los tratados indica que esa lista no es exhaustiva y que pueden incorporarse motivos de naturaleza comparable. Estos motivos adicionales se reconocen generalmente cuando reflejan la experiencia de grupos sociales vulnerables que han sido marginados en el pasado o que lo son en la actualidad¹⁵. El Comité de Derechos Económicos, Sociales y Culturales, por ejemplo, ha reconocido como motivos protegidos la edad, la nacionalidad, el estado civil y familiar, la orientación sexual y la identidad de género, la discapacidad, el estado de salud y la situación económica y social¹⁶. Tanto las formas directas como indirectas de trato diferencial pueden constituir una discriminación prohibida.

12. El artículo 20, párrafo 2, del Pacto Internacional de Derechos Civiles y Políticos establece que toda apología del odio nacional, racial o religioso que constituya incitación a la discriminación, la hostilidad o la violencia estará prohibida por la ley. Los artículos 19 y 20 del Pacto se complementan entre sí. El artículo 19, párrafo 3, establece que toda restricción del derecho a la libertad de expresión deberá estar fijada por la ley y ser necesaria para asegurar el respeto a los derechos o a la reputación de los demás y la protección de la seguridad nacional, el orden público o la salud o la moral públicas¹⁷.

13. Las empresas tienen la obligación de respetar los derechos humanos, lo que significa que deben abstenerse de infringir los derechos humanos de terceros y hacer frente a las consecuencias negativas sobre los derechos humanos en las que tengan alguna participación, de conformidad con los Principios Rectores sobre las Empresas y los Derechos Humanos¹⁸. Los Principios Rectores exigen a las empresas que detecten, prevengan y mitiguen las consecuencias negativas sobre los derechos que se deriven de sus operaciones comerciales o estén relacionadas con ellas, y reflejan las obligaciones de los Estados de proteger contra las violaciones de los derechos humanos cometidas por empresas dentro de su jurisdicción y de garantizar el acceso a una reparación efectiva cuando se produzcan abusos.

14. En un número creciente de resoluciones, la Asamblea General y el Consejo de Derechos Humanos han reconocido que los efectos discriminatorios de la datificación de las sociedades plantean un grave desafío a los derechos humanos¹⁹. Los riesgos de discriminación en el contexto de la inteligencia artificial se reconocen en el Pacto Digital Global, que contiene el compromiso de elaborar normas sobre datos y metadatos diseñadas para prevenir y abordar los sesgos, la discriminación o las violaciones y los abusos de los derechos humanos durante todo el ciclo de vida de los datos (véase el párr. 42 *infra*).

B. Otros marcos internacionales pertinentes

15. En respuesta a las capacidades cada vez mayores de las tecnologías basadas en datos, se han desarrollado numerosos marcos jurídicos para la recopilación y el tratamiento de datos. Entre ellos figuran la Convención de la Unión Africana sobre Ciberseguridad y Protección de Datos Personales y el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal del Consejo de Europa. Además, en muchos Estados se han aprobado leyes nacionales de protección de datos, aunque siguen existiendo lagunas considerables.

¹⁴ Comité de Derechos Económicos, Sociales y Culturales, observación general núm. 20 (2009), párr. 13.

¹⁵ *Ibid.*, párr. 27.

¹⁶ *Ibid.*, párrs. 27 a 35.

¹⁷ Comité de Derechos Humanos, observación general núm. 34 (2011), relativa a la libertad de opinión y la libertad de expresión, párr. 50.

¹⁸ Véase la resolución 17/4 del Consejo de Derechos Humanos.

¹⁹ Véanse las resoluciones de la Asamblea General 78/187, 78/213 y 78/265 y la resolución 54/21 del Consejo de Derechos Humanos.

16. La discriminación y la desigualdad se abordan en estos y otros marcos relacionados con los datos de varias maneras, entre ellas otorgando a determinadas categorías de datos - cuyo tratamiento conlleva mayores riesgos de discriminación- un mayor grado de protección²⁰. Otros instrumentos prohíben directamente la discriminación a través del tratamiento de datos²¹.

17. Los esfuerzos recientes se han centrado en la creación de marcos jurídicos para la inteligencia artificial. La igualdad y la no discriminación son preocupaciones centrales abordadas en tales marcos, como el Convenio Marco del Consejo de Europa sobre Inteligencia Artificial y Derechos Humanos, Democracia y Estado de Derecho y leyes a nivel regional y nacional, como el Reglamento de Inteligencia Artificial de la Unión Europea y la Ley Básica de Desarrollo de la Inteligencia Artificial y Establecimiento de la Confianza de la República de Corea²². La Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura ha adoptado una recomendación sobre la ética de la inteligencia artificial, en la que se subraya la importancia de la no discriminación en el uso responsable de la inteligencia artificial.

III. El papel de los datos como fuente de discriminación y desigualdad

A. Efectos dispares en ámbitos clave

18. La sección III contiene una descripción de las principales cuestiones relativas al papel de los datos como fuente de discriminación y desigualdad en sectores clave. Cabe señalar que surgen problemas similares en sectores que van más allá de los abordados en el presente informe, así como en contextos de conflicto armado; el límite de extensión de este informe imposibilita el poder analizarlos.

19. A menudo surgen problemas cuando los sistemas automatizados de toma de decisiones, los análisis predictivos y los sistemas de reconocimiento biométrico incorporan sesgos o se emplean en contextos que hacen probable que singularicen o afecten desproporcionadamente a determinados grupos. Los sistemas de reconocimiento biométrico, por ejemplo, incluidos los de reconocimiento facial, tienen problemas de precisión patentes, en función del tono de la piel y del sexo. Aunque los desarrolladores puedan mitigar esos resultados²³, persisten otros problemas. Históricamente, las tecnologías de vigilancia se han desplegado de forma que afectan desproporcionadamente a las comunidades marginadas y con bajos ingresos, y a veces se utilizan para atacar a determinados grupos²⁴. Los sistemas de reconocimiento biométrico proporcionan la información necesaria para elaborar perfiles de las personas en función de su etnia, raza, género y otras características personales²⁵. También se han utilizado sistemas de reconocimiento biométrico para identificar y rastrear a manifestantes pacíficos y disidentes, lo que equivale a discriminación por motivos de opinión política. El despliegue de una tecnología de vigilancia tan potente también puede desalentar

²⁰ Véanse la Convención de la Unión Africana sobre Ciberseguridad y Protección de Datos Personales y la versión revisada del Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal del Consejo de Europa (Protocolo de Enmienda, Serie de Tratados del Consejo de Europa, núm. 223).

²¹ Véanse la Ley General de Protección de Datos del Brasil, los Principios rectores sobre la reglamentación de los ficheros computadorizados de datos personales y los Principios sobre Protección y Privacidad de los Datos Personales. Véase también [ST/SGB/2024/3](#).

²² Véase <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>; y https://cset.georgetown.edu/wp-content/uploads/t0625_south_korea_ai_law_EN.pdf. Muchos otros Estados están debatiendo proyectos de ley relacionados con la inteligencia artificial; véase la comunicación de Colombia.

²³ Véase https://pages.nist.gov/frvt/reports/demographics/nistir_8429.pdf.

²⁴ Véase <https://www.aclu.org/documents/aclu-comment-facial-recognition-and-biometric-technologies-eo-14074-13e>; y las comunicaciones de Access Now y Human Rights Myanmar.

²⁵ Véanse [A/HRC/44/57](#), párrs. 39 y 40; y [A/HRC/48/31](#).

el ejercicio de las libertades públicas y otros derechos²⁶. Algunos informes anteriores del Alto Comisionado contienen un análisis más detallado de estas cuestiones²⁷.

1. Aplicación de la ley y justicia penal

20. La policía y los tribunales utilizan cada vez más herramientas de predicción basadas en datos²⁸. Entre ellas se incluyen herramientas con las que predecir dónde pueden producirse delitos y sistemas para determinar el riesgo de reincidencia o señalar a personas como riesgos o probables sospechosos. Estos sistemas dependen de grandes cantidades de datos, como datos históricos y en tiempo real, antecedentes penales, registros de detenciones, estadísticas de delincuencia, registros de intervenciones policiales en lugares concretos, publicaciones y metadatos de medios sociales, datos de comunicaciones y datos de localización. Está bien documentado que los resultados de estos sistemas suelen mostrar importantes sesgos, a menudo como consecuencia de sesgos históricos en los sistemas de aplicación de la ley y de justicia penal, que afectan negativamente a las minorías raciales, étnicas y religiosas en particular²⁹. Esto se suma a las preocupaciones derivadas del uso del reconocimiento biométrico, como se ha mencionado anteriormente.

2. Migración

21. Las personas que se desplazan son a menudo objeto de prácticas de recopilación y tratamiento de datos especialmente generalizadas e intrusivas, con graves implicaciones para los derechos humanos. La infraestructura para gestionar la migración depende cada vez más de amplias tecnologías basadas en datos, como la inteligencia artificial, los sistemas algorítmicos automatizados de toma de decisiones, el análisis predictivo y las tecnologías digitales relacionadas³⁰. Estas tecnologías pueden utilizarse para muchos fines, entre ellos la detección en las fronteras físicas, la determinación de riesgos definidos por el Estado en evaluaciones algorítmicas de riesgos³¹, la verificación de identidades y la gestión de la presencia de migrantes en un país. Los datos recopilados, almacenados, procesados y compartidos pueden incluir datos biométricos, datos sanitarios, datos de medios sociales, logros educativos, situación laboral, nacionalidad, datos de localización, información sobre redes personales y profesionales, situación familiar, antecedentes penales, datos financieros y datos sobre actividades políticas y de otro tipo. Los datos se recogen de las personas afectadas, organismos estatales, empresas privadas, incluidos los intermediarios de datos, organizaciones internacionales y otros Estados. Los gobiernos han ido creando sistemas y bases de datos cada vez más integrados e interoperables, lo que permite el acceso a los datos a un gran número de organismos para una amplia gama de fines³². A partir de estos sistemas y bases de datos, las autoridades determinan quién puede entrar en un país o debe salir y quién puede tener acceso a prestaciones y servicios. Aunque esos objetivos son legítimos, los efectos adversos suelen afectar desproporcionadamente a personas de determinados orígenes nacionales o étnicos debido, por ejemplo, a los prejuicios integrados en los sistemas de

²⁶ Véanse A/HRC/44/24, A/HRC/48/31 y A/HRC/51/17; y la comunicación de Pete Fussey y Daragh Murray. Véanse también A/HRC/48/76 y A/75/590.

²⁷ A/HRC/44/24, A/HRC/48/31 y A/HRC/51/17.

²⁸ Véase A/79/296.

²⁹ Véase Comité para la Eliminación de la Discriminación Racial, recomendación general núm. 36 (2020), relativa a la prevención y la lucha contra la elaboración de perfiles raciales por los agentes del orden. Véase también el documento de sesión del Consejo de Derechos Humanos titulado “Promoción y protección de los derechos humanos y las libertades fundamentales de los africanos y los afrodescendientes frente al uso excesivo de la fuerza y otras violaciones de los derechos humanos por agentes del orden”, párr. 93, disponible en el sitio web del Consejo (<https://www.ohchr.org/es/hr-bodies/hrc/regular-sessions/session47/list-reports>).

³⁰ Véanse A/HRC/48/76 y A/75/590.

³¹ Estas tecnologías pueden comprender incluso sistemas pseudocientíficos de reconocimiento de emociones que no son capaces de procesar los matices culturales o de otra índole y que pueden incluso incorporar en sus procesos postulados eugenésicos de la frenología. Véanse también A/HRC/48/31 y la comunicación de Access Now.

³² Véanse <https://www.ohchr.org/sites/default/files/2023-09/Digital-Border-Governance-A-Human-Rights-Based-Approach.pdf>; y la comunicación de AsyLex.

adopción de decisiones basada en datos y, en ocasiones, a las prácticas discriminatorias de aplicación de perfiles³³.

3. Prestaciones sociales

22. Las tecnologías basadas en datos se están convirtiendo en un elemento cada vez más central de la forma en que los Estados gestionan y prestan servicios esenciales, entre ellos la asistencia social y la salud pública. Entre los objetivos de estos sistemas figuran el aumento de la eficiencia, la prestación precisa de servicios y la detección del fraude. Se utilizan para determinar la admisibilidad a los programas y los importes de las prestaciones, hacer cumplir los límites de ingresos y bienes y verificar la identidad. También se despliegan para señalar situaciones en las que es necesario intervenir, por ejemplo cuando pueden producirse situaciones de abuso. Existe un gran potencial para aprovechar la toma de decisiones y el apoyo algorítmico a fin de avanzar hacia objetivos tan importantes. El Relator Especial sobre la extrema pobreza y los derechos humanos ha señalado, por ejemplo, que la automatización de las prestaciones podría ser una forma clave de abordar la no percepción de las prestaciones sociales, ya que podría reducir la complejidad administrativa para los posibles beneficiarios³⁴.

23. Existen riesgos significativos para la igualdad en el disfrute del derecho a la privacidad y otros derechos. El acceso a los servicios sociales se ha relacionado a menudo con el deterioro de las garantías de privacidad de las personas con bajos ingresos, ya que se espera que los solicitantes y beneficiarios proporcionen amplia información sobre su vida privada, lo que puede llegar a incluir medidas intrusivas. Este fenómeno afecta desproporcionadamente a las mujeres y a los miembros de minorías raciales o étnicas y puede perpetuarse gracias a las tecnologías digitales³⁵. Un antiguo Relator Especial sobre la extrema pobreza y los derechos humanos se refirió a la utilización de la contrastación de datos sin restricciones para exponer, vigilar y castigar a los beneficiarios de la asistencia social como una potencial “distopía de bienestar digital”³⁶.

24. Los datos utilizados proceden en parte de los solicitantes, en parte de otras fuentes, como diversas bases de datos gubernamentales y medios sociales, o se compran a proveedores comerciales³⁷. El uso de sistemas algorítmicos de toma de decisiones o de apoyo puede dar lugar al corte de una fuente principal de ingresos, la denegación del acceso a tratamiento médico y la denegación de una vivienda básica; incluso puede desencadenar investigaciones y procesos penales. La denegación de prestaciones puede tener efectos negativos de gran alcance en la vida de las personas, como la insolvencia, la pérdida de la vivienda y el deterioro de la salud. Como consecuencia, es posible que las personas más necesitadas de ayuda no se beneficien de la automatización, sino que queden excluidas³⁸. Dados los riesgos de tales impactos negativos, es esencial que los sistemas sean especialmente fiables y estén sujetos a una supervisión minuciosa.

25. Sin embargo, hay muchos informes de sistemas algorítmicos utilizados en el contexto de las prestaciones sociales que se habían diseñado incorrectamente, eran inexactos o sencillamente erróneos y se utilizaban de forma profundamente discriminatoria. Por ejemplo, el Auditor General del estado de Michigan (Estados Unidos de América) revisó 22.000 avisos de fraude de un sistema automatizado de detección adoptado por el sistema estatal de seguro de desempleo y descubrió que el 93 % de ellos no implicaba realmente fraude³⁹. Los sistemas automatizados de verificación de la identidad que dejan en suspenso las solicitudes de

³³ Véase <https://www.ohchr.org/sites/default/files/2023-09/Digital-Border-Governance-A-Human-Rights-Based-Approach.pdf>.

³⁴ Véase A/HRC/50/38.

³⁵ Véase Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (Nueva York, St. Martin's Press, 2017); y Khiara M. Bridges, *The Poverty of Privacy Rights* (Redwood City, California, Stanford Law Books, 2017).

³⁶ Véase A/74/493.

³⁷ A/HRC/48/31, párr. 30.

³⁸ Véase A/HRC/50/38 y Sebastian Smart, “Algorithmic discrimination in Latin American welfare States”, documento de debate del Carr Center, núm. 2024-05 (Cambridge, Massachusetts, Escuela Kennedy de Harvard, 2024).

³⁹ Tribunal de Apelaciones de los Estados Unidos, *Cahoo et al. v. SAS Analytics Inc. et al.*, núm. 18-1296 (Sexto Circuito, 2019).

prestaciones, a veces durante meses o años, han provocado que miles de personas vulnerables renuncien a ellas o reciban pagos reducidos, al tiempo que sobrecargan al personal con un trabajo de verificación adicional⁴⁰. La comprobación sustitutiva de medios de vida, a menudo utilizada para permitir evaluaciones automatizadas cuando no hay acceso a datos individualizados, ha suscitado críticas por no captar las realidades de la pobreza y la vulnerabilidad con todos sus matices. En varios entornos, se han documentado altos niveles de errores de exclusión e inclusión; en algunos programas, los errores de exclusión han alcanzado valores de hasta el 70 % y el 93 %⁴¹.

4. Salud

26. La digitalización de los servicios sanitarios tiene un gran potencial para mejorar de manera directa la vida de las personas. Al reducir la necesidad de evaluación física, la atención virtual ofrece oportunidades para llegar a comunidades remotas y otras personas que se enfrentan a barreras en el acceso físico a los establecimientos de salud. El uso de la inteligencia artificial y el aprendizaje automático ha permitido analizar grandes conjuntos de datos para tareas de predicción, previsión, desarrollo de fármacos y vacunas y diagnóstico médico⁴².

27. Al mismo tiempo, las aplicaciones de salud digital afectan a algunos de los aspectos más íntimos y sensibles de la vida de las personas, lo que atañe a dimensiones fundamentales de la privacidad. Como ha señalado la Relatora Especial sobre el derecho de toda persona al disfrute del más alto nivel posible de salud física y mental, las tecnologías de salud digital pueden perpetuar el capacitismo, el racismo, el sexismo o la discriminación por motivos de orientación sexual o identidad de género, entre otros⁴³. Por ejemplo, las herramientas y aplicaciones médicas pueden funcionar de forma diferente en función de factores como el tono de la piel, el origen étnico, la edad y el sexo. Una revisión encargada por el Gobierno del Reino Unido de Gran Bretaña e Irlanda del Norte halló indicios de que los dispositivos dotados de inteligencia artificial utilizados para diagnosticar el cáncer de piel podrían tener peores resultados en pacientes con tonos de piel más oscuros y suscitó preocupación por el infradiagnóstico de cardiopatías en mujeres y de glaucoma en personas de ascendencia asiática⁴⁴. La gestión de casos médicos basada en la inteligencia artificial también puede mostrar sesgos marcados. Uno de estos productos, utilizado con más de 200 millones de personas en hospitales para predecir qué pacientes tendrían más probabilidades de necesitar atención médica adicional, señaló a los pacientes de piel clara con mucha más frecuencia que a los pacientes negros con un estado de salud comparable⁴⁵.

28. Múltiples estudios han indicado que los datos de salud, incluidos los recopilados a través de aplicaciones de salud móvil, se comparten a menudo sin el consentimiento o incluso el conocimiento de las personas afectadas. Esto es especialmente preocupante cuando la información incluye la identidad de género, la sexualidad, la ubicación o el estado de salud, inclusive cuando dicha información puede deducirse de otros datos. Las mujeres que buscan atención de la salud reproductiva pueden estar expuestas a riesgos particulares⁴⁶. Por ejemplo, una amplia gama de aplicaciones sanitarias recogen grandes cantidades de datos que pueden estar a disposición de las fuerzas del orden en jurisdicciones en las que el aborto está penalizado⁴⁷. Otras aplicaciones, como las de citas, han sido vectores de investigación y criminalización de las personas LGBTQI+⁴⁸. Las compañías de seguros médicos pueden

⁴⁰ Kevin De Liban, *Inescapable AI: The Ways AI Decides How Low-Income People Work, Live, Learn, and Survive* (Los Ángeles, TechTonic Justice, 2024), pág. 59.

⁴¹ Véase Smart, “Algorithmic discrimination”.

⁴² Véase A/HRC/53/65.

⁴³ *Ibid.*

⁴⁴ Véase <https://www.gov.uk/government/publications/equity-in-medical-devices-independent-review-final-report>. Véase también la comunicación de Privacy International.

⁴⁵ Véase Ziad Obermeyer y otros, “Dissecting racial bias in an algorithm used to manage the health of populations”, *Science*, vol. 366, núm. 6464 (octubre de 2019).

⁴⁶ Véanse las comunicaciones de AI & Equality y Asociación para el Progreso de las Comunicaciones.

⁴⁷ Véase la comunicación de Privacy International.

⁴⁸ Véase Gwen Aviles, “Tinder introduces safety feature to protect LGBTQ travelers”, NBC News, 24 de julio de 2019; y la comunicación de ILGA Asia.

obtener acceso a datos de salud o genéticos sensibles, por ejemplo mediante la compra de datos a corredores de datos, y emplearlos para denegar la cobertura o una atención esencial basándose en el estado de salud o incluso simplemente en el estado de salud potencial⁴⁹.

5. Infraestructura pública digital

29. En los últimos años han cobrado un notable impulso los esfuerzos de los Estados por desplegar sistemas digitales fundamentales, incluidos sistemas de identidad y pago, que permitan la prestación a escala de servicios esenciales en ámbitos como el bienestar, la sanidad, la educación y las finanzas. Estos sistemas tienen un gran potencial para facilitar una mayor inclusión, pero también pueden constituir un obstáculo para el disfrute de los derechos humanos o incluso contribuir a violaciones y abusos de los derechos⁵⁰. Como capa clave para permitir las transacciones de datos intensivos entre dominios, la infraestructura pública digital puede facilitar la vigilancia arbitraria. Debido a la escala y la naturaleza de los datos acumulados, cualquier violación de acceso a los datos puede afectar a la sociedad de manera profunda. También existen pruebas fehacientes de los efectos discriminatorios y excluyentes asociados a las infraestructuras públicas digitales, en particular los sistemas de identificación digitalizados⁵¹.

30. Tales efectos pueden materializarse de diversas maneras. Por ejemplo, puede haber obstáculos considerables para inscribirse en los sistemas de identificación, como procesos de registro costosos o difíciles, la imposibilidad de llegar a zonas remotas y a personas desplazadas y apátridas, la existencia de costumbres y prácticas que sean desfavorables para grupos minoritarios o para mujeres y niñas, y el temor entre sectores vulnerables de la población a que el sistema se utilice contra ellos. El diseño del sistema y los fallos técnicos también pueden contribuir a resultados dispares, como las opciones de diseño no inclusivas (por ejemplo, categorías de datos que no se corresponden con la autoidentificación) y la falta de conectividad estable a Internet. Los factores que intervienen en el uso de la infraestructura pública digital también pueden contribuir sustancialmente a generar resultados desiguales, entre ellos los requisitos de identificación excesivos, la proliferación de funciones (es decir, la expansión de los requisitos de uso a sectores inicialmente imprevistos) y la falta de acceso o reconocimiento de medios alternativos de identificación.

6. Vigilancia

31. Como se ha destacado en informes anteriores, una serie de actividades de vigilancia llevadas a cabo tanto por los Estados como por las empresas constituyen importantes amenazas para el derecho a la privacidad y otros derechos humanos. La mayoría de las actividades públicas y muchas privadas pueden controlarse, cuantificarse y analizarse. Las cámaras de vigilancia son omnipresentes en muchos lugares y cada vez están más equipadas con tecnología de reconocimiento biométrico. Las llamadas ciudades inteligentes se están implantando en todas las regiones del mundo, creando sistemas muy complejos de recopilación y tratamiento constante de datos, habilitados por sensores cada vez más avanzados. Los espacios en línea están sometidos a una vigilancia constante por parte de autoridades y empresas que recopilan cantidades ingentes de información sobre los internautas, elaboran perfiles de las personas y analizan las redes. Estos datos pueden utilizarse con fines legítimos e ilegítimos, incluso en situaciones de conflicto. Cada vez se presta más atención a la forma en que se utilizan en los conflictos armados los datos recopilados y procesados, entre otros mediante vigilancia, y a las graves repercusiones que ello tiene sobre la población civil y los bienes de carácter civil⁵². Se puede abusar de la

⁴⁹ Véase Casey Ross y Bob Herman, “Denied by AI: how Medicare Advantage plans use algorithms to cut off care for seniors in need”, *STAT*, 13 de marzo de 2023; y Marshall Allen, “Health insurers are vacuuming up details about you - and it could raise your rates”, *ProPublica*, 17 de julio de 2018.

⁵⁰ Véase el Marco Universal de Salvaguardias de la Infraestructura Pública Digital para obtener orientación sobre una serie de salvaguardias contra las violaciones de derechos y otros riesgos, disponible en <https://www.dpi-safeguards.org/es>.

⁵¹ Véanse A/HRC/43/29 y la comunicación de Access Now.

⁵² Véase Russell Buchan y Asaf Lubin, eds., “The rights to privacy and data protection in times of armed conflict”, *Revista Internacional de la Cruz Roja*, vol. 105, núm. 923 (junio de 2023); y

vigilancia ubicua para la elaboración de perfiles raciales y para identificar y rastrear a personas con fines discriminatorios, por ejemplo debido a sus creencias políticas. Incluso cuando se usa para objetivos legítimos, desde la gestión de entornos urbanos complejos hasta la facilitación del acceso a los servicios públicos, dicha vigilancia no suele cumplir el requisito de proporcionalidad. Plantea un serio desafío al derecho a la privacidad y a las libertades que constituyen el núcleo de las sociedades abiertas y democráticas⁵³.

7. Información en línea

32. El entorno de la información en línea está configurado por procesos basados en datos, que pueden contribuir a resultados discriminatorios. Un importante estudio de los motores de búsqueda puso de manifiesto la existencia generalizada de resultados racistas⁵⁴, aspecto preocupante que también se refleja en otras formas de expresión discriminatoria y de odio. La selección de contenidos en los medios sociales se basa en grandes cantidades de datos recopilados sobre cada usuario, lo que puede incluir una selección discriminatoria. Se ha denunciado que los anunciantes pueden, en algunas plataformas, seleccionar a su público objetivo según criterios que, al menos indirectamente, se corresponden con motivos prohibidos, por ejemplo excluyendo a miembros de determinados grupos raciales o étnicos de ver anuncios de vivienda o empleo o dirigiendo deliberadamente a personas vulnerables productos con los que se puede sacar partido de ellas, como juegos de azar y préstamos⁵⁵. Los algoritmos de selección centrados en la interacción, que seleccionan contenidos basándose en datos sobre patrones de navegación anteriores, también pueden conducir a la amplificación de la incitación al odio y los contenidos xenófobos. Al mismo tiempo, los estudios han revelado que la moderación automática de contenidos, incluidos los sistemas de detección de discursos de odio, puede estar sesgada y, por tanto, limitar desproporcionadamente los contenidos de miembros de minorías⁵⁶. Estos sistemas tienden a ser especialmente poco fiables, y potencialmente perjudiciales, respecto a las lenguas no dominantes⁵⁷. También se ha demostrado que los generadores de imágenes de inteligencia artificial generativa producen resultados con un alto grado de prejuicios⁵⁸.

B. Retos comunes

1. Cuestiones relacionadas con los sistemas y su diseño

a) Diseño técnico y toma de decisiones

33. El trato desigual puede tener su origen en el proceso de diseño de un sistema basado en datos, empezando por las primeras decisiones sobre lo que se supone que debe conseguir y cómo se medirá⁵⁹. Si el objetivo, por ejemplo, es optimizar el despliegue de la policía mediante la predicción de altos índices de delincuencia, los tipos de delitos que se incluyan influirán en quién se verá afectado; por ejemplo, los delitos contra la propiedad pueden ser cometidos más a menudo por personas pobres, mientras que el fraude fiscal es un delito asociado a la riqueza.

Robin Geiss y Henning Lahmann, "Protection of data in armed conflict", documento de trabajo, Academia de Derecho Internacional Humanitario y Derechos Humanos de Ginebra, febrero de 2021.

⁵³ Véase [A/HRC/51/17](#).

⁵⁴ Véase Safiya Umoja Noble, *Algorithms of Oppression* (Nueva York, New York University Press, 2018).

⁵⁵ Véase <https://verfassungsblog.de/targeted-ad>; y la comunicación de AI & Equality.

⁵⁶ Véase <https://aclanthology.org/P19-1163.pdf>.

⁵⁷ Véase <https://ecnl.org/publications/algorithmic-gatekeepers-impacts-llm-content-moderation-civic-space-and-human-rights>.

⁵⁸ Véase Ananya, "AI image generators often give racist and sexist results: can they be fixed?", *Nature*, 19 de marzo de 2024.

⁵⁹ Véase Solon Barocas y Andrew D. Selbst, "Big data's disparate impact", *California Law Review*, vol. 104, núm. 3 (junio de 2016); y Agencia de Cooperación Policial de la Unión Europea (Europol), *AI Bias in Law Enforcement: A Practical Guide* (Luxemburgo, Oficina de Publicaciones de la Unión Europea, 2025), págs. 22 a 50.

34. La calidad de los datos utilizados para desarrollar y utilizar tecnologías basadas en datos puede ser otro problema importante. A menudo, los conjuntos de datos utilizados están viciados por inexactitudes y categorizaciones discriminatorias. Por ejemplo, una investigación sobre un conjunto de datos ampliamente utilizado para el entrenamiento de sistemas de visión artificial reveló innumerables casos de categorización arbitraria, incoherencias y categorizaciones claramente racistas, misóginas o con carácter de odio y discriminación; en última instancia, el operador de la base de datos eliminó 600.000 imágenes⁶⁰. El carácter incompleto y la falta de representatividad de los datos son los principales vectores que motivan los resultados dispares de los sistemas algorítmicos⁶¹. Por ejemplo, los grupos históricamente desfavorecidos suelen estar infrarrepresentados o sobrerrepresentados en los conjuntos de datos, lo que sesga cualquier análisis de la muestra. Un sistema de predicción policial que utilice datos históricos de detenciones que puedan reflejar prácticas policiales con sesgo racial habituales en el pasado plantea el riesgo de orientar las predicciones futuras en la misma dirección sesgada. Esto, a su vez, puede llevar a un exceso de vigilancia en el futuro, lo que provocará más detenciones de personas del mismo grupo y creará así un peligroso bucle de retroalimentación⁶². La suposición común de que los datos son representativos rara vez está justificada y quizá sea más a menudo incorrecta que correcta⁶³. Además, los datos que pueden ser adecuados en determinados contextos pueden no serlo para otros. Por ejemplo, si un modelo se entrenara con los registros de delincuencia de un Estado en el que un determinado tipo de delito tuviera una alta prevalencia, fallaría en otro en el que ese delito pudiera ser menos común⁶⁴.

35. Otra cuestión relacionada es el uso de indicadores indirectos y su efecto en los resultados de los sistemas algorítmicos. Aunque se tenga cuidado de que un conjunto de datos no incluya datos directos sobre características protegidas, otros datos pueden servir de indicadores de dichas características⁶⁵. Por ejemplo, los códigos postales o determinados nombres de pila pueden correlacionarse con la pertenencia a un grupo y convertirse así en indicadores indirectos que sesgan el análisis de los datos en detrimento de las personas afectadas.

b) Transparencia y rendición de cuentas

36. Las herramientas basadas en datos plantean retos sin precedentes en lo que respecta a la transparencia de la toma de decisiones y la rendición de cuentas por las mismas. Predominan dos retos. En primer lugar, los gobiernos y los agentes privados no suelen facilitar información adecuada sobre sus productos, servicios y herramientas basados en datos. Las personas afectadas por estos sistemas y el público en general a menudo no pueden saber cuándo los sistemas basados en datos toman decisiones que les afectan, y mucho menos cómo. En tales circunstancias, es difícil, cuando no imposible, examinar con detenimiento la adopción de decisiones basada en datos. En segundo lugar, el entorno de datos, los algoritmos y los modelos son inmensamente complejos. Los resultados de los sistemas de aprendizaje automático, incluidos los grandes modelos lingüísticos, suelen ser difíciles o imposibles de explicar, un fenómeno que suele denominarse como el problema de la “caja negra”⁶⁶. En consecuencia, la rendición de cuentas en los casos en que tales sistemas causan daños sigue siendo difícil, por ejemplo cuando una persona perjudicada debe demostrar la culpa y la causalidad en sus reclamaciones por daños y perjuicios. Esto, a su vez, limita los incentivos

⁶⁰ Véase <https://excavating.ai>; y <https://image-net.org/update-sep-17-2019>.

⁶¹ Véase Barocas y Selbst, “Big data's disparate impact”.

⁶² Comité para la Eliminación de la Discriminación Racial, recomendación general núm. 36 (2020), párr. 33.

⁶³ Véase Barocas y Selbst, “Big data's disparate impact”.

⁶⁴ Arvind Narayanan y Sayash Kapoor, *AI Snake Oil: What Artificial Intelligence Can Do, What It Can't, and How to Tell the Difference* (Princeton, Nueva Jersey, Princeton University Press, 2024), pág. 52.

⁶⁵ Véase Barocas y Selbst, “Big data's disparate impact”; y Europol, *AI Bias in Law Enforcement*, págs. 24 y 32.

⁶⁶ Véase Ariel Bleicher, “Demystifying the black box that is AI”, *Scientific American*, 9 de agosto de 2017. No obstante, estos sistemas no tienen por qué ser totalmente inescrutables; véase <https://doi.org/10.1145/3351095.3372873>.

para que los desarrolladores, operadores y usuarios de sistemas automatizados basados en datos actúen de forma legal y no discriminatoria.

c) Escalabilidad

37. La escalabilidad de las herramientas basadas en datos puede amplificar drásticamente los efectos negativos de las tasas de error y sesgo, incluso cuando estos son reducidos⁶⁷. Los problemas arraigados en tales sistemas pueden abarcar a cientos, miles o incluso millones de personas. Esa es una diferencia clave con respecto a los prejuicios individuales.

d) Inferencias y predicciones

38. La capacidad de las aplicaciones basadas en datos para hacer inferencias y predicciones conlleva riesgos considerables. Datos aparentemente inocuos, a menudo ni siquiera relacionados con una persona concreta, se utilizan ampliamente para predecir el comportamiento humano, sacar conclusiones sobre el mundo interior de las personas, sus intereses, opiniones y rasgos de carácter, y determinar características personales sensibles, como el estado de salud y la orientación sexual. Estas inferencias y predicciones pueden dar lugar a decisiones que afecten a los derechos de las personas, a veces de forma totalmente automatizada⁶⁸. Por ejemplo, los historiales de navegación pueden revelar información sobre la vida sexual, el estado de salud o las opiniones políticas de alguien, lo que a su vez podría utilizarse para denegar la cobertura de un seguro médico o convertir a alguien en objeto de persecución política. Se necesitan urgentemente salvaguardias adecuadas contra estas prácticas, entre otras cosas actualizando la legislación pertinente, como las leyes de protección de datos, de lucha contra la discriminación, de protección del consumidor y sectoriales⁶⁹.

2. Sesgos humanos, estructurales e institucionales

39. Los riesgos y daños provocados por los datos afectan regularmente a las personas marginadas y en situación de vulnerabilidad. Los efectos adversos diferenciados sufridos por los miembros de determinados grupos son a menudo concurrentes, y la discriminación y la exclusión solo pueden percibirse y abordarse plenamente mediante un enfoque intersectorial⁷⁰. Por ejemplo, la discriminación basada en la situación socioeconómica a menudo se cruza con la discriminación racial o étnica. Las mujeres periodistas se enfrentan a campañas de acoso en línea con una frecuencia desproporcionadamente mayor que sus homólogos masculinos, y de formas muy específicas centradas en el género.

40. El sesgo sistémico suele reflejar prejuicios y suposiciones humanas profundamente arraigadas, incluidas las que se arrastran durante períodos más largos. El racismo y el sexismo institucionales son ejemplos comunes. Este sesgo puede perpetuarse, por ejemplo, en la decisión de desplegar determinadas herramientas digitales en contextos en los que es mucho más probable que afecten a poblaciones históricamente desfavorecidas. Está bien documentado, por ejemplo, que las tecnologías de vigilancia intrusiva y otras herramientas de uso intensivo de datos se dirigen de forma desproporcionada contra las minorías o los migrantes⁷¹. Un amplio conjunto de investigaciones señala que los estereotipos (por ejemplo, que los parados no quieren trabajar o que los extranjeros son delincuentes) y las posturas

⁶⁷ [A/HRC/48/31](#), párr. 18.

⁶⁸ Véase [A/HRC/48/31](#).

⁶⁹ *Ibid.* y comunicación de Privacy International.

⁷⁰ Véase la resolución 78/187 de la Asamblea General; Comité para la Eliminación de la Discriminación contra la Mujer, recomendaciones generales núm. 35 (2017), relativa a la violencia por razón de género contra la mujer, por la que se actualiza la recomendación general núm. 19, y núm. 39 (2022), relativa a los derechos de las mujeres y las niñas indígenas; Comité para la Eliminación de la Discriminación Racial, recomendación general núm. 36 (2020); y Red de las Naciones Unidas sobre discriminación racial y protección de las minorías, *Guidance Note on Intersectionality, Racial Discrimination and Protection of Minorities* (Ginebra, ACNUDH, 2022). Véanse también las comunicaciones de la Asociación para el Progreso de las Comunicaciones y de Media Monitoring Africa.

⁷¹ Véase ACNUDH y Universidad de Essex, “Digital border governance: a human rights-based approach”, septiembre de 2023; y [A/75/590](#).

ideológicas (por ejemplo, que la pobreza es un fracaso moral individual) son un trasfondo común de tales decisiones⁷².

41. Si bien algunos de estos sesgos pueden filtrarse inconscientemente en diversas decisiones relativas al diseño, la implantación y el funcionamiento de los sistemas de tratamiento de datos, en ocasiones la discriminación, en contravención del derecho internacional de los derechos humanos, puede ser el objetivo mismo de dichos sistemas. Por ejemplo, los sistemas podrían discriminar directamente identificando a los disidentes mediante análisis automáticos de las publicaciones en los medios sociales o centrándose en determinadas comunidades religiosas para someterlas a una vigilancia sistémica.

42. A veces, la supuesta objetividad de los datos y de las herramientas basadas en datos esconde prácticas profundamente injustas tanto en la prestación de servicios públicos como en la oferta de productos y servicios en el mercado. En ocasiones, las tecnologías nuevas, no probadas o sin fundamento científico se despliegan primero entre personas que carecen de los medios y la capacidad para oponerse a tales despliegues, como los migrantes o las personas con bajos ingresos⁷³. Las tecnologías basadas en datos también se han utilizado como poderosas herramientas de opresión al permitir la identificación, vigilancia y censura de defensores de los derechos humanos, manifestantes y disidentes.

3. El papel del sector privado

43. El papel dominante del sector privado para impulsar el desarrollo y la implantación de tecnología plantea retos particulares. Las empresas tienen la responsabilidad de respetar los derechos humanos en todas sus operaciones, mientras que los Estados tienen el deber de velar por que las empresas no cometan violaciones de derechos humanos⁷⁴. Los Principios Rectores sobre las Empresas y los Derechos Humanos instan a los Estados a aplicar una combinación inteligente de las medidas normativas y políticas de que disponen para velar por que no se produzcan daños a los derechos humanos en relación con los productos y servicios de las empresas tecnológicas, incluidas las medidas normativas y las orientaciones, incentivos y requisitos de transparencia que las acompañan.

44. La aplicación exhaustiva de ese marco plantea innumerables retos en el contexto de las tecnologías digitales. Las prácticas de recopilación y tratamiento de datos por parte de las empresas son a menudo excesivas y están relacionadas con la discriminación, y los Estados se enfrentan a numerosos obstáculos para ofrecer una protección efectiva. La falta de capacidad para evaluar plenamente la oferta del sector privado, por ejemplo, puede perjudicar a algunos agentes estatales. La presión para crear un entorno empresarial favorable y competitivo puede limitar la voluntad de los Estados de implantar las medidas de protección necesarias para abordar los problemas de derechos humanos⁷⁵.

45. Estos retos pueden ser especialmente graves cuando existe un estrecho nexo entre el Estado y las empresas en el desarrollo y el funcionamiento de las herramientas basadas en datos, como cuando los Estados recurren a proveedores privados o establecen alianzas público-privadas. En tales contextos, existe el riesgo de que se difuminen las responsabilidades entre el Estado y los agentes privados, especialmente cuando las cadenas de suministro son largas y complejas. Cuando los Estados apoyan económicamente a las empresas tecnológicas, las contratan o se abastecen de ellas, deben tomar medidas activas para garantizar que las empresas con las que trabajan respetan los derechos humanos. Los Estados deberían utilizar su posición para insistir en una conducta empresarial basada en los derechos y en la entrega de productos que no conduzcan a una discriminación ilegal. Deberían supervisar el desarrollo y despliegue de los sistemas basados en datos que adquieran y exigir y evaluar información sobre los conjuntos de datos y la exactitud y riesgos de la aplicación. Cuando los riesgos no puedan mitigarse eficazmente, los Estados no deberían

⁷² Véase Eubanks, *Automating Inequality*; Bridges, *The Poverty of Privacy Rights*; y Noble, *Algorithms of Oppression*.

⁷³ A/75/590, párrs. 38 a 42.

⁷⁴ Véase <https://www.ohchr.org/sites/default/files/Documents/Issues/Business/B-Tech/b-tech-foundational-paper-state-duty-to-protect.pdf>.

⁷⁵ Véanse A/HRC/59/32 y A/HRC/59/53.

utilizar, desplegar ni autorizar los productos en cuestión⁷⁶. Deberían prohibirse las aplicaciones que no puedan funcionar de conformidad con el derecho internacional de los derechos humanos⁷⁷.

4. Brechas digitales

46. La discriminación y la desigualdad basadas en los datos reflejan a menudo pautas persistentes de exclusión de la participación en la esfera digital. En 2024, casi un tercio de la población mundial no tenía acceso a Internet, y la tasa de conectividad solo alcanzaba el 27 % en los países de ingreso bajo. Las diferencias entre hombres y mujeres persisten y son especialmente pronunciadas en los países de ingreso bajo y medio-bajo. También existe una marcada brecha de acceso entre las zonas rurales y las urbanas. Por lo general, la pobreza implica un menor acceso a Internet⁷⁸. También existen grandes disparidades en la alfabetización digital y las competencias digitales en función de la ubicación, la situación socioeconómica, el género y otros factores. Los mercados de trabajo en los sectores digitales siguen estando marcados por las disparidades de género. Por ejemplo, las mujeres solo representan aproximadamente el 30 % de la fuerza de trabajo dedicada a la inteligencia artificial⁷⁹.

47. Las aplicaciones digitales parecen desarrollarse a menudo con el objetivo de dirigirse a regiones y audiencias que prometen grandes beneficios. Algunas soluciones digitales pueden no estar al alcance de las personas que viven en países de ingreso bajo o medio, personas con discapacidad, minorías o pueblos indígenas, entre otros, o ser inasequibles o de mala calidad para contextos determinados⁸⁰.

48. El predominio de determinadas lenguas en muchos productos y servicios digitales también impide que las personas, a menudo las mencionadas en el párrafo anterior, tengan acceso a ellos. Las interfaces de usuario y las políticas de los medios sociales están disponibles en un número limitado de idiomas. La falta de asistencia lingüística aumenta el riesgo de uso inadecuado de los datos, ya que afecta a la capacidad de los usuarios para comprender y ajustar la configuración de privacidad y seguridad⁸¹. El rendimiento de las ofertas dominantes de inteligencia artificial generativa es sistemáticamente alto en muy pocas lenguas. Estas limitaciones afectan a miles de millones de usuarios y pueden limitar su participación en el discurso político, la cultura y la esfera económica. Cuando determinadas lenguas no disponen de recursos en línea, no se tiene en cuenta una gran cantidad de información. Ello puede afectar a la configuración de los futuros productos y servicios y contribuir a que las políticas adoptadas como respuesta sean inadecuadas. Cabe señalar que grandes esfuerzos comunitarios han dado lugar al desarrollo de sitios web, herramientas, recursos y una serie de modelos lingüísticos para lenguas de escasos recursos⁸²; los futuros trabajos para ampliar el alcance digital de las lenguas deberían potenciar esos esfuerzos.

49. Además, muchos Estados carecen de marcos normativos suficientes, incluidas leyes de protección de datos, e incluso cuando existen, las autoridades pueden tener una capacidad limitada para hacerlas cumplir eficazmente, especialmente en mercados de bajos ingresos⁸³. Ello deja a las personas de esas regiones especialmente expuestas a violaciones y abusos de los derechos humanos, incluidas las prácticas discriminatorias en materia de datos. Si bien muchos Estados han mejorado sus marcos normativos, políticas y prácticas en los últimos

⁷⁶ Véase A/HRC/48/31.

⁷⁷ *Ibid.* Véase también la resolución 78/213 de la Asamblea General.

⁷⁸ Véase https://www.itu.int/hub/publication/D-IND-ICT_MDD-2024-4; y

<https://pulse.internetsociety.org/en/blog/exploring-the-global-state-of-internet-poverty-in-2024>.

⁷⁹ Véase Comité para la Eliminación de la Discriminación contra la Mujer, recomendación general núm. 40 (2024), relativa a la representación igualitaria e inclusiva de las mujeres en los sistemas de toma de decisiones; y <https://www.randstad.com/randstad-ai-equity>.

⁸⁰ Véanse las comunicaciones de Guatemala y Montenegro.

⁸¹ Véase Nyalleng Moorosi, "Better data sets won't solve the problem - we need AI for Africa to be developed in Africa", *Nature*, vol. 636, núm. 8042 (diciembre de 2024).

⁸² Véase <https://tehiku.nz/te-hiku-tech>; y <https://theconversation.com/how-ai-could-help-safeguard-indigenous-languages-255359>.

⁸³ Véase la comunicación de la Asociación para el Progreso de las Comunicaciones.

años, es necesario redoblar los esfuerzos para garantizar que el derecho a la privacidad se defienda por igual en todas las regiones⁸⁴.

IV. Conclusiones y recomendaciones

50. La creciente dependencia de las tecnologías basadas en datos, incluida la inteligencia artificial, ha provocado importantes y crecientes transformaciones en las sociedades y ha operado cambios en las economías, los entornos políticos y las culturas. Estos avances han introducido nuevos y complejos retos para el disfrute de los derechos a la privacidad y a la no discriminación y la igualdad. La recopilación y el tratamiento de datos, sobre todo cuando se utilizan para tomar decisiones automatizadas, pueden perpetuar y exacerbar las desigualdades y las prácticas discriminatorias existentes, y ya lo están haciendo a gran escala. Quienes tienen más probabilidades de ser víctimas de esos procesos suelen ser las personas ya marginadas y las personas en situación de vulnerabilidad.

51. La innovación tecnológica debe anclarse en el derecho y las normas internacionales de derechos humanos. La discriminación y la desigualdad no son cuestiones marginales; son fallos sistémicos que comprometen la integridad de las sociedades, la gobernanza democrática y participativa y la realización de los derechos humanos para todos. Teniendo en cuenta la velocidad a la que se están desplegando las tecnologías basadas en datos y la magnitud de los daños que pueden acarrear, estas cuestiones deben abordarse con la máxima urgencia, desde el ámbito local al mundial. En este contexto, los signos de la creciente oposición al establecimiento de salvaguardias para el desarrollo de tecnologías basadas en datos bajo el argumento de que fomentan la innovación son profundamente preocupantes. Se necesitan sólidas salvaguardias y orientaciones en materia de derechos humanos para hacer posible una innovación que funcione para todos.

52. Las tecnologías basadas en datos reflejan las desigualdades estructurales que impregnan las realidades sociales, económicas y políticas. Abordar estas cuestiones requiere un enfoque global e interseccional que va más allá del alcance del presente informe. No obstante, existen medidas concretas y aplicables que los Estados, las empresas y otras partes interesadas deberían adoptar. Muchas recomendaciones clave se han expuesto en informes anteriores del Alto Comisionado y en resoluciones del Consejo de Derechos Humanos⁸⁵. Lo que sigue debe leerse en conjunción con dichas recomendaciones. Además, las medidas recomendadas no deberían considerarse de forma aislada, sino que deberían formar parte de un esfuerzo sostenido y global de toda la sociedad.

53. El ACNUDH recomienda a los Estados:

a) Establecer marcos normativos que aborden exhaustivamente la discriminación y la desigualdad que se producen en el contexto de la recopilación y el tratamiento de datos. Estos marcos no deberían basarse en enfoques aislados y deberían incluir legislación específica sobre protección de datos, privacidad, libertad de información, lucha contra la discriminación, inteligencia artificial y normativa sectorial. Los Estados deberían garantizar que las excepciones que establezca la legislación nacional no afecten negativamente al disfrute de los derechos humanos ni den lugar a violaciones de los mismos, como las excepciones generales para la aplicación de la ley, la gestión de la migración o la seguridad nacional;

b) Proteger a las personas de los abusos de derechos humanos vinculados a la recopilación y el tratamiento de datos por parte de las empresas mediante la

⁸⁴ Véase <https://techpoint.africa/news/worldcoin-delete-biometric-data-kenya>. Véanse también las comunicaciones de Guatemala y Media Monitoring Africa.

⁸⁵ A/HRC/44/24, A/HRC/48/31, A/HRC/51/17, A/HRC/53/42 y A/HRC/59/32; y las resoluciones del Consejo de Derechos Humanos 50/15, 54/21 y 59/11

aplicación de una combinación inteligente de medidas reguladoras y políticas de incentivos:

c) Garantizar capacidades efectivas de supervisión y aplicación, entre otras cosas mediante la creación y dotación adecuada de autoridades independientes e imparciales de protección de datos, organismos de lucha contra la discriminación y supervisión sectorial;

d) Utilizar siempre las herramientas basadas en datos respetando plenamente el derecho internacional de los derechos humanos, incluidos los derechos a la privacidad, a la igualdad y a un recurso efectivo y la prohibición de la discriminación, y garantizar que toda limitación de los derechos humanos se ajuste a los principios de legalidad, necesidad y proporcionalidad;

e) Condicionar la contratación de tecnologías, productos y servicios basados en datos al pleno cumplimiento de las normas de no discriminación;

f) Garantizar que las infraestructuras públicas digitales se diseñan, despliegan, explotan y utilizan de forma que se respeten los derechos a la privacidad, la no discriminación y la igualdad, estableciendo normas de privacidad y seguridad de los datos que sean plenamente compatibles con el derecho internacional, creando sólidas salvaguardias jurídicas, operativas, procedimentales y tecnológicas para evitar el abuso de tales sistemas, incluso para la vigilancia ilegal o arbitraria, limitando el tipo de información contenida, quién tiene acceso a ella y cómo se utiliza, y garantizando la inclusión y la plena accesibilidad para todos;

g) Abstenerse de condicionar el acceso a los servicios públicos, incluidas las prestaciones sociales, la atención de la salud y la educación básica, a la identificación digital sin permitir medios de identificación alternativos;

h) Garantizar el estricto cumplimiento del derecho internacional de los derechos humanos, incluidos los principios de necesidad y proporcionalidad, cuando se considere el uso de tecnologías biométricas, por ejemplo para el funcionamiento de infraestructuras públicas digitales y en contextos policiales⁸⁶;

i) Garantizar que las víctimas de violaciones y abusos de los derechos humanos, incluidos los derechos a la no discriminación y a la igualdad, relacionados con prácticas indebidas de recopilación, tratamiento y uso de datos puedan acceder a recursos efectivos. Con ese objetivo, y dada la gravedad de los daños potenciales, considerar la posibilidad de establecer o ampliar los servicios de asistencia jurídica y apoyo a las víctimas que sean necesarios en esos contextos;

j) Adoptar urgentemente todas las medidas necesarias para combatir la brecha digital dentro de los países y entre ellos, entre otros acelerando los esfuerzos internacionales, regionales y nacionales encaminados a construir la infraestructura necesaria para proveer un acceso universal y eficaz a Internet, promoviendo contenidos locales en todos los idiomas pertinentes y mejorando la alfabetización digital;

k) Mejorar la cooperación internacional, la creación de capacidad, la asistencia técnica y la investigación para que todos los países puedan desarrollar, desplegar y regular las tecnologías basadas en datos según las necesidades de sus poblaciones, sobre la base de los derechos humanos;

l) Facilitar el diálogo y el debate sobre las tecnologías basadas en datos y su regulación en los procesos intergubernamentales y de múltiples partes interesadas existentes y futuros, inclusive en el contexto del Pacto Digital Global y el proceso de la Cumbre Mundial sobre la Sociedad de la Información, con vistas a promover los derechos humanos y el desarrollo sostenible.

⁸⁶ Para obtener más detalles sobre la tecnología de reconocimiento biométrico a distancia, incluida la recomendación de una moratoria, al menos hasta que se hayan establecido suficientes salvaguardias, véanse [A/HRC/44/24](#), párr. 53 j), incisos i) a v); [A/HRC/48/31](#), párr. 59 d); y [A/HRC/51/17](#), párrs. 56 g) y 57 d).

54. El ACNUDH recomienda a los Estados y las empresas:

a) Aplicar sistemáticamente la diligencia debida en materia de derechos humanos a lo largo de todo el ciclo de vida de los sistemas basados en datos que diseñen, desarrollen, implanten, vendan, obtengan o exploten, prestando especial atención a los efectos discriminatorios y de otra índole de dichos sistemas. Un elemento fundamental de la diligencia debida en materia de derechos humanos debería ser la realización de evaluaciones periódicas y exhaustivas de los efectos de estos sistemas sobre tales derechos;

b) Aumentar drásticamente la transparencia en el uso de sistemas automatizados de adopción de decisiones basada en datos, en particular informando adecuadamente al público y a las personas afectadas, permitiendo que se realicen auditorías independientes y externas de los sistemas automatizados y supervisando sistemáticamente dichos sistemas y sus repercusiones, en colaboración con las partes interesadas pertinentes. Cuanto más probables y graves sean los efectos adversos potenciales o reales sobre los derechos humanos, más necesaria será la transparencia;

c) Garantizar que los trabajadores responsables del desarrollo y despliegue de tecnologías basadas en datos y los empleados que utilicen dichas herramientas sean sensibles a los problemas de discriminación y desigualdad y tengan la capacidad de abordar adecuadamente dichos problemas. Esto incluye tomar medidas decisivas para garantizar la diversidad de los trabajadores y llevar a cabo medidas de concienciación y capacitación, como la formación en la lucha contra todas las formas de discriminación, incluidos los prejuicios implícitos y la discriminación sistémica, para todos los implicados en el diseño, desarrollo y despliegue de la inteligencia artificial;

d) Garantizar la participación sustantiva de todas las partes interesadas en las decisiones sobre el desarrollo, la implantación y el uso de los sistemas basados en datos, en particular de las personas y grupos afectados.

55. El ACNUDH recomienda además a las empresas:

a) Hacer todo lo posible para cumplir con su responsabilidad de respetar los derechos humanos, incluso mediante la plena operatividad de los Principios Rectores sobre las Empresas y los Derechos Humanos, centrándose en la lucha contra la discriminación vinculada al desarrollo, la venta o la explotación de productos y servicios basados en datos;

b) Aprobar una declaración de intención que establezca su planteamiento para respetar el derecho a la privacidad y evitar los efectos discriminatorios de la recopilación y el tratamiento de datos;

c) Supervisar la eficacia de las acciones destinadas a mitigar los efectos discriminatorios y consultar periódicamente a los grupos afectados;

d) Proporcionar mecanismos efectivos de reclamación a nivel operacional para los productos y servicios digitales, participando activamente en ellos, y ofrecer recursos efectivos a las personas y comunidades afectadas, también en cooperación con los mecanismos judiciales estatales, cuando dichos productos o servicios hayan causado o contribuido a causar impactos adversos sobre los derechos humanos, incluida la discriminación.

56. El ACNUDH recomienda que las organizaciones de normalización elaboren y apliquen normas para luchar contra la discriminación en el tratamiento de datos en procesos abiertos que incluyan todas las medidas necesarias para garantizar la participación de todas las partes interesadas pertinentes, incluidos los miembros de los grupos afectados, basándose en las recomendaciones expuestas en el informe del ACNUDH sobre los derechos humanos y los procesos de establecimiento de normas técnicas para las tecnologías digitales nuevas y emergentes⁸⁷.

⁸⁷ A/HRC/53/42.

57. Todas las partes interesadas pertinentes deberían adoptar medidas proactivas y sostenidas para identificar, prevenir y mitigar el sesgo en los datos y los sistemas algorítmicos, entre otras cosas:

a) Invertir en investigación y desarrollo de metodologías para detectar, mitigar y eliminar los sesgos en los conjuntos de datos y los modelos;

b) Mejorar las prácticas de recopilación de datos para reducir el sesgo sistémico en origen, por ejemplo garantizando que los procesos de recopilación de datos sean inclusivos y representativos de poblaciones diversas e implicando a las comunidades afectadas en las decisiones sobre qué datos se recopilan y cómo se etiquetan y utilizan;

c) Institucionalizar la mitigación de sesgos en los flujos de trabajo de desarrollo, por ejemplo integrando sistemáticamente las evaluaciones de impacto;

d) Fomentar la colaboración interdisciplinar y el intercambio de conocimientos, entre otras cosas promoviendo la colaboración entre tecnólogos, sociólogos, especialistas en ética y expertos en derechos humanos.
