Naciones Unidas A/HRC/RES/54/21

Asamblea General

Distr. general
16 de octubre de 2023
Español
Original: inglés

Consejo de Derechos Humanos
54º período de sesiones
11 de septiembre a 13 de octubre de 2023
Tema 3 del programa
Promoción y protección de todos los derechos humanos, civiles, políticos, económicos, sociales y culturales, incluido el derecho al desarrollo

Resolución aprobada por el Consejo de Derechos Humanos el 12 de octubre de 2023

54/21. El derecho a la privacidad en la era digital

El Consejo de Derechos Humanos,

Guiado por los propósitos y principios de la Carta de las Naciones Unidas,

Reafirmando los derechos humanos y las libertades fundamentales consagrados en la Declaración Universal de Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos, el Pacto Internacional de Derechos Económicos, Sociales y Culturales y otros instrumentos internacionales de derechos humanos pertinentes,

Recordando todas las resoluciones anteriores de la Asamblea General y del Consejo de Derechos Humanos sobre el derecho a la privacidad en la era digital, así como otras resoluciones pertinentes,

Acogiendo con beneplácito la labor de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos sobre el derecho a la privacidad en la era digital, y acogiendo con beneplácito también la labor de varios titulares de mandatos de procedimientos especiales del Consejo de Derechos Humanos sobre el derecho a la privacidad y sus contribuciones a la promoción y protección del derecho a la privacidad,

Reafirmando el derecho humano a la privacidad, según el cual nadie debe ser objeto de injerencias arbitrarias o ilícitas en su vida privada, su familia, su domicilio o su correspondencia, y el derecho a la protección de la ley contra tales injerencias, y reconociendo que el ejercicio del derecho a la privacidad es importante para materializar otros derechos humanos, como el derecho a la libertad de expresión y a abrigar opiniones sin injerencias, y el derecho a la libertad de reunión y de asociación pacíficas, y es una de las bases de una sociedad democrática,

Reconociendo que el derecho a la privacidad está intrínsecamente ligado a la protección efectiva de los datos personales de cada individuo,

Reconociendo también que el derecho a la privacidad puede permitir el disfrute de otros derechos, el libre desarrollo de la personalidad y la identidad de las personas, y su capacidad para participar en la vida política, económica, social y cultural,

Reafirmando que los derechos que las personas tienen fuera del entorno virtual también deben estar protegidos en este, incluido el derecho a la privacidad, y señalando que la sincronización acelerada de los ámbitos en línea y tradicionales puede afectar a las personas, incluido su derecho a la privacidad,

Observando que los procesos de adopción de decisiones algorítmicos o automatizados en línea pueden afectar al disfrute de los derechos de las personas en otros ámbitos,

Reconociendo la necesidad de seguir debatiendo y analizando, sobre la base del derecho internacional de los derechos humanos, las cuestiones relativas a la promoción y protección del derecho a la privacidad en la era digital, las garantías procesales, la supervisión y los recursos nacionales efectivos, y el efecto de la vigilancia en el disfrute del derecho a la privacidad y otros derechos humanos, así como la necesidad de examinar los principios de no arbitrariedad, licitud, legalidad, necesidad y proporcionalidad en relación con las prácticas de vigilancia, y de considerar los efectos potencialmente discriminatorios,

Observando que el rápido ritmo del desarrollo tecnológico permite a las personas de todo el mundo utilizar la tecnología de la información y las comunicaciones y, al mismo tiempo, incrementa la capacidad de los Gobiernos, las empresas y las personas para llevar a cabo actividades de vigilancia, interceptación, piratería informática y recopilación de datos, lo que podría constituir una violación o una transgresión de los derechos humanos, en particular del derecho a la privacidad, y que, por lo tanto, esta cuestión suscita cada vez más preocupación,

Observando también que las violaciones y las transgresiones del derecho a la privacidad en la era digital pueden afectar a todas las personas y tener repercusiones particulares en las mujeres, los niños y las niñas, las personas con discapacidad y las personas de edad, así como las personas en situaciones vulnerables y los grupos marginados, y que el tratamiento de los datos personales debe estar sujeto a salvaguardias y restricciones en materia de derechos humanos, especialmente los datos de las personas en situaciones vulnerables,

Observando además que las mujeres y las niñas experimentan violaciones y transgresiones de su derecho a la privacidad por motivos de género, tanto en línea como en otros ámbitos, así como violaciones o transgresiones que tienen repercusiones en función del género, y reconociendo que la forma en que muchas plataformas digitales se diseñan, comercializan, mantienen y rigen puede dar lugar a desinformación, información errónea y discursos de odio, lo que puede exacerbar los estereotipos de género, dar lugar a violencia sexual y de género y socavar la protección de datos y el cumplimiento de todos los derechos de las mujeres y las niñas, en particular su derecho a la privacidad,

Observando que los niños pueden ser particularmente vulnerables a las transgresiones y violaciones de su derecho a la privacidad, en particular mediante el ciberacoso, el ciberacecho y el abuso y la explotación sexuales, y observando también que los Estados Partes deben aplicar la Convención sobre los Derechos del Niño en relación con el entorno digital, incluida la importancia de la privacidad para la autonomía, la dignidad y la seguridad de los niños y para el ejercicio de sus derechos,

Reconociendo la necesidad de la diligencia debida en materia de derechos humanos en los procesos de concepción, diseño, utilización, adquisición, transferencia, venta, despliegue y ulterior desarrollo de tecnologías nuevas y emergentes, como las que entrañan el uso de inteligencia artificial, ya que pueden, sin las salvaguardias adecuadas, repercutir en el disfrute del derecho a la privacidad y otros derechos humanos, y que los riesgos para estos derechos pueden y deben evitarse o reducirse al mínimo, entre otras cosas adoptando medidas para garantizar una infraestructura de datos sin riesgos, transparente, responsable, segura y de gran calidad, ejerciendo la diligencia debida y la revisión periódica de las tecnologías ya implantadas para evaluar, prevenir y mitigar las repercusiones negativas sobre los derechos humanos, y proporcionando recursos efectivos, incluidos recursos judiciales y mecanismos de reparación, y estableciendo la supervisión humana,

Reconociendo que, pese a sus efectos positivos, el uso de tecnologías digitales y de sistemas de inteligencia artificial que requieren el procesamiento de una gran cantidad de datos, a menudo datos personales sobre, entre otras cosas, el comportamiento, las relaciones

sociales, las preferencias privadas y la identidad de una persona, incluidos los metadatos, puede entrañar graves riesgos para el derecho a la privacidad, en particular cuando se emplea para la identificación, el rastreo, la elaboración de perfiles, el reconocimiento facial, la predicción de la conducta o la aplicación de sistemas de puntuación de las personas,

Observando que la utilización de la extracción de datos y de algoritmos para orientar los contenidos hacia los usuarios en línea puede socavar la capacidad de actuación del usuario y el acceso a la información en línea, así como el derecho a la libertad de opinión y expresión, y puede propiciar que se intensifiquen las amenazas de la información errónea, la desinformación y el discurso de odio, en particular en las plataformas de medios sociales, lo que puede desembocar en actos de violencia, incluida la violencia política, y recordando a este respecto el Plan de Acción de Rabat sobre la prohibición de la apología del odio nacional, racial o religioso que constituye incitación a la discriminación, la hostilidad o la violencia,

Observando con preocupación la intrusión y el impacto de las prácticas de recopilación de datos, las repercusiones y los daños conexos derivados de la vigilancia y el creciente uso de algoritmos relacionados con la aplicación de sistemas de inteligencia artificial,

Observando con preocupación también que determinados algoritmos predictivos y el uso cada vez mayor de tecnologías de reconocimiento facial y vigilancia pueden dar lugar a discriminación, en particular cuando los datos utilizados en el entrenamiento de los algoritmos no son precisos, pertinentes y representativos y no se verifican para evitar sesgos encubiertos,

Observando que el uso de la inteligencia artificial, sin las debidas salvaguardias en materia de derechos humanos, puede plantear el riesgo de reforzar la discriminación, incluidas las desigualdades estructurales, especialmente durante el procesamiento de datos sensibles, y reconociendo que en la concepción, el desarrollo, la aplicación y el uso de las tecnologías digitales nuevas y emergentes deben evitarse los resultados discriminatorios desde el punto de vista racial o desde cualquier otro punto de vista,

Observando con preocupación la existencia de informes que indican una menor precisión de la identificación mediante datos biométricos, incluidas las tecnologías de reconocimiento facial que presentan sesgos y prejuicios raciales en detrimento de las mujeres, entre otras cosas cuando se usan datos de entrenamiento no representativos, y que la utilización de las tecnologías digitales puede reproducir, reforzar e incluso exacerbar las desigualdades raciales y por razón de género, y reconociendo la importancia que revisten en este contexto los recursos efectivos,

Reconociendo que, si bien los metadatos pueden aportar beneficios, algunos tipos de metadatos, tomados en conjunto, pueden revelar información personal que puede ser tan sensible como el propio contenido de las comunicaciones y dar indicación del comportamiento, incluidos los movimientos, las relaciones sociales, las actividades políticas, las preferencias privadas y la identidad de una persona, y recordando en consecuencia que los proveedores de servicios deben tomar medidas para reducir al mínimo, ocultar o eliminar los metadatos y para reducir la trazabilidad de los metadatos de los usuarios con el fin de reforzar las protecciones que ofrece el cifrado y proteger el derecho a la privacidad,

Reconociendo que la falta de acceso a tecnologías y servicios asequibles y confiables sigue siendo un problema fundamental en muchos países en desarrollo, especialmente para superar las brechas digitales, entre los países y dentro de ellos, y la brecha digital de género, y para avanzar en el desarrollo en sus diversas formas, incluido el logro de los Objetivos de Desarrollo Sostenible, y subrayando a este respecto que muchos Estados de todo el mundo, incluidos países en desarrollo, necesitan apoyo para superar estas brechas digitales y alcanzar los Objetivos de Desarrollo Sostenible,

Reconociendo también la necesidad de garantizar el respeto del derecho internacional de los derechos humanos, entre otros mediante la realización de evaluaciones del impacto en los derechos humanos relativas a las fases de concepción, diseño, desarrollo, despliegue, evaluación y regulación de las tecnologías basadas en datos y a los procesos de establecimiento de normas técnicas, y de garantizar que dichas tecnologías estén sujetas a las salvaguardias y la supervisión adecuadas,

Expresando preocupación porque con frecuencia las personas, en particular los niños, no dan o no pueden dar su consentimiento libre, explícito e informado a la recopilación, el procesamiento y el almacenamiento de sus datos o para la reutilización, venta o reventa múltiple de sus datos personales, ya que la recogida, el tratamiento, el uso, el almacenamiento y el intercambio de datos personales, incluidos los datos sensibles, han aumentado considerablemente en la era digital, y que si se divulgan datos personales y sensibles, pueden causarse daños, perjuicios o dificultades notables a las personas,

Observando en particular que la vigilancia de las comunicaciones digitales debe ser compatible con las obligaciones internacionales en materia de derechos humanos y debe llevarse a cabo sobre la base de un marco jurídico que sea de acceso público, claro, preciso, amplio y no discriminatorio, y que toda injerencia en el derecho a la privacidad debe atenerse a los principios de legalidad, necesidad y proporcionalidad, teniendo en cuenta lo que sea razonable en relación con la persecución de objetivos legítimos, y recordando que los Estados que son partes en el Pacto Internacional de Derechos Civiles y Políticos deben adoptar las medidas necesarias para aprobar las leyes u otras disposiciones que hagan falta a fin de hacer efectivos los derechos reconocidos en el Pacto,

Observando con profunda preocupación que, en muchos países, hay personas y organizaciones que promueven y defienden los derechos humanos y las libertades fundamentales, periodistas y otros trabajadores de los medios de difusión que, como resultado de sus actividades, pueden sufrir con frecuencia amenazas, acoso e inseguridad, así como injerencias ilegales o arbitrarias en su derecho a la privacidad,

Observando con profunda preocupación también el uso de herramientas tecnológicas desarrolladas por la industria de la vigilancia privada y por actores privados o públicos para llevar a cabo la vigilancia, la piratería informática de dispositivos y sistemas (entre otros mediante el uso de programas maliciosos o espía), la interceptación y la interrupción de las comunicaciones, y la recopilación de datos, interfiriendo en la vida profesional y privada de las personas, incluidas las que se dedican a la promoción y defensa de los derechos humanos y las libertades fundamentales, los periodistas y otros trabajadores de los medios de comunicación, en violación o transgresión de sus derechos humanos, específicamente del derecho a la privacidad,

Recordando que las empresas comerciales, incluidas las tecnológicas, tienen la responsabilidad de respetar los derechos humanos establecidos en los Principios Rectores sobre las Empresas y los Derechos Humanos: Puesta en Práctica del Marco de las Naciones Unidas para “Proteger, Respetar y Remediar”, y que la obligación y la responsabilidad primordial de promover y proteger los derechos humanos y las libertades fundamentales incumben al Estado, y acogiendo con beneplácito la labor de la Oficina del Alto Comisionado sobre la aplicación de estos principios respecto a las tecnologías digitales,

Poniendo de relieve que, en la era digital, es importante contar con soluciones técnicas para asegurar y proteger la confidencialidad de las comunicaciones digitales, incluidas medidas de cifrado, uso de seudónimos y anonimato, a fin de garantizar el disfrute de los derechos humanos, en particular los derechos a la privacidad, la libertad de opinión y expresión y la libertad de reunión y de asociación pacíficas, y reconociendo que los Estados deben promover estas medidas y abstenerse de recurrir a técnicas de vigilancia ilícitas o arbitrarias, que podrían incluir formas de piratería informática y restricciones del acceso y el uso de las tecnologías de cifrado,

Subrayando la necesidad de garantizar que las medidas de seguridad nacional y de salud pública, incluido el uso de la tecnología para vigilar y contener la propagación de enfermedades infecciosas, cumplan plenamente las obligaciones de los Estados con arreglo al derecho internacional de los derechos humanos y respeten los principios de licitud, legalidad y legitimidad en relación con el objetivo que se persigue, necesidad y proporcionalidad, y la necesidad de proteger los derechos humanos, incluido el derecho a la privacidad, así como de proteger los datos personales en la respuesta a emergencias sanitarias o de otro tipo, y subrayando también la necesidad de suprimir o anonimizar los datos recogidos una vez que hayan dejado de cumplir los fines para los que se recogieron,

1. *Reafirma* el derecho a la privacidad, según el cual nadie debe ser objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, y el derecho a la protección de la ley contra tales injerencias, establecidos en el artículo 12 de la Declaración Universal de Derechos Humanos y el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos;

2. *Recuerda* que los Estados deben asegurar que toda injerencia en el derecho a la privacidad se ajuste a los principios de legalidad, necesidad y proporcionalidad;

3. *Recuerda también* la creciente repercusión que tienen las tecnologías nuevas y emergentes, como las surgidas en los ámbitos de la vigilancia, la inteligencia artificial, la adopción automatizada de decisiones y el aprendizaje automático, así como la elaboración de perfiles, el rastreo y la biometría, incluido el reconocimiento facial, cuando no cuentan con las debidas salvaguardias en materia de derechos humanos respecto al pleno disfrute del derecho a la privacidad y otros derechos humanos, y reconoce que algunas aplicaciones podrían no ser compatibles con el derecho internacional de los derechos humanos;

4. *Afirma* que los derechos que las personas tienen fuera del entorno virtual también deben estar protegidos en este, incluido el derecho a la privacidad;

5. *Afirma también* que, para proteger, respetar y promover el derecho a la privacidad, los datos personales solo deben recogerse con fines determinados, explícitos y legítimos, y deben tratarse de forma lícita, justa y transparente;

6. *Resalta* que toda persona debe poder verificar qué autoridades públicas o qué particulares u organismos privados controlan o pueden controlar sus datos personales, y que cualquier injerencia en la protección de datos debe ser lícita, de conformidad con el derecho internacional de los derechos humanos, incluidos los principios de legalidad, proporcionalidad, necesidad y no discriminación;

7. *Reconoce* que los riesgos para el derecho a la privacidad y otros derechos humanos pueden y deben reducirse al mínimo mediante la adopción de normativas o de otros mecanismos apropiados, de conformidad con las obligaciones aplicables en virtud del derecho internacional de los derechos humanos, durante los procesos de concepción, diseño, utilización, adquisición, transferencia, venta, despliegue y desarrollo ulterior de tecnologías nuevas y emergentes como la inteligencia artificial, garantizando una infraestructura de datos sin riesgos, segura y de gran calidad, ejerciendo la diligencia debida para evaluar, prevenir y mitigar las repercusiones negativas sobre los derechos humanos, y estableciendo la supervisión humana, así como mecanismos de reparación;

8. *Destaca* que los Estados deben cumplir con sus obligaciones en materia de derechos humanos y que las empresas, incluidas las tecnológicas, deben respetar el derecho a la privacidad y otros derechos humanos cuando recopilen, procesen, compartan y almacenen datos personales, entre otras cosas, adoptando políticas y salvaguardias de protección de datos;

9. *Destaca también* que los sistemas de vigilancia biométrica a distancia, incluidos los de reconocimiento facial, suscitan gran preocupación en cuanto a su proporcionalidad, dado su carácter altamente invasivo y sus amplias repercusiones en un gran número de personas;

10. *Exhorta* a todos los Estados a que:

a) Respeten y protejan el derecho a la privacidad, incluso en el contexto de las comunicaciones digitales y las tecnologías nuevas y emergentes;

b) Adopten medidas para poner fin a las violaciones y transgresiones del derecho a la privacidad y creen las condiciones necesarias para impedirlas, como cerciorarse de que la legislación nacional pertinente se ajusta a sus obligaciones en virtud del derecho internacional de los derechos humanos, en particular en el caso de personas en situación vulnerable o grupos marginados;

c) Revisen periódicamente sus procedimientos, prácticas y legislación en relación con la vigilancia de las comunicaciones, entre otras cosas la vigilancia en gran escala y la interceptación y recopilación de datos personales, así como en relación con la utilización de perfiles, la adopción automatizada de decisiones, el aprendizaje automático y las tecnologías biométricas, a fin de defender el derecho a la privacidad, lo que entraña que se garantice el cumplimiento cabal y efectivo de todas las obligaciones contraídas en virtud del derecho internacional de los derechos humanos;

d) Respeten las obligaciones internacionales en materia de derechos humanos, inclusive en lo referente al derecho a la privacidad, cuando intercepten las comunicaciones digitales de las personas o recopilen datos personales, cuando compartan los datos reunidos, entre otras cosas, mediante acuerdos de intercambio de información o den acceso a esos datos por otros medios, y cuando exijan a terceros, incluidas las empresas, la divulgación de datos personales;

e) Velen por que todas las medidas adoptadas para luchar contra el terrorismo y el extremismo violento conducente al terrorismo que interfieran con el derecho a la privacidad se ajusten a los principios de legalidad, necesidad y proporcionalidad, y cumplan las obligaciones que les incumben en virtud del derecho internacional;

f) Garanticen que las tecnologías de identificación y reconocimiento biométrico, incluidas las tecnologías de reconocimiento facial por parte de agentes públicos y privados, no permitan la vigilancia arbitraria o ilegal, entre otros de quienes ejercen su derecho a la libertad de reunión pacífica;

g) Garanticen que los programas de identidad digital o biométrica se diseñen, apliquen y operen tras la adopción de salvaguardias técnicas, reglamentarias, jurídicas y éticas adecuadas y respetando plenamente las obligaciones de los Estados en virtud del derecho internacional de los derechos humanos;

h) Elaboren o mantengan y apliquen una legislación adecuada, con sanciones y recursos eficaces, que proteja a las personas contra las violaciones y las transgresiones del derecho a la privacidad, concretamente las que se producen mediante la recopilación, el procesamiento, la retención o la utilización de datos personales por particulares, Gobiernos, empresas y organizaciones privadas sin el consentimiento libre, explícito e informado de los interesados o de cualquier otra manera que no sea legal, de conformidad con el derecho internacional de los derechos humanos;

i) Consideren la posibilidad de adoptar o mantener leyes, normas y políticas de protección de datos, incluidos los datos de las comunicaciones digitales, que se ajusten a sus obligaciones internacionales en materia de derechos humanos, que podrían incluir disposiciones sobre la protección de datos personales sensibles y el establecimiento de autoridades nacionales independientes con las facultades y los recursos necesarios para supervisar las prácticas de protección de datos, investigar las violaciones y transgresiones y recibir comunicaciones de particulares y organizaciones, y ofrecer vías de recurso eficaces;

j) Consideren la posibilidad de aprobar o revisar leyes, reglamentos o políticas para asegurarse de que todas las empresas, incluidas las de medios sociales y otras plataformas en línea, incorporen plenamente el derecho a la privacidad y otros derechos humanos pertinentes cuando conciban, desarrollen, desplieguen y evalúen tecnologías, incluida la inteligencia artificial, adopten las medidas adecuadas para mejorar y alentar la rendición de cuentas corporativa y proporcionen a las personas cuyos derechos hayan sido violados o transgredidos acceso a un recurso efectivo que comprenda la reparación y garantías de no repetición;

k) Sigan elaborando o manteniendo a ese respecto medidas preventivas y vías de recurso para las violaciones y transgresiones del derecho a la privacidad en la era digital, que pueden afectar a todas las personas, entre otras situaciones cuando tengan repercusiones particulares para las mujeres, los niños y las niñas y las personas en situaciones vulnerables o los grupos marginados;

l) Elaboren, examinen, apliquen y fortalezcan políticas y programas con perspectiva de género que contribuyan al empoderamiento de todas las mujeres y las niñas y promuevan y protejan el derecho de todas las personas a la privacidad en la era digital;

m) Proporcionen una orientación eficaz y actualizada a las empresas sobre la forma de respetar los derechos humanos asesorándolas sobre métodos apropiados, incluida la diligencia debida en materia de derechos humanos, y sobre la manera de considerar eficazmente las cuestiones de género, vulnerabilidad o marginación, y consideren la posibilidad de tomar medidas apropiadas para que las empresas puedan adoptar medidas voluntarias de transparencia adecuadas en relación con las solicitudes de las autoridades estatales que requieran acceso a datos e información de carácter privado de los usuarios;

n) Se abstengan de utilizar las tecnologías de vigilancia de una manera que no cumpla con las obligaciones internacionales en materia de derechos humanos, inclusive cuando se utilizan contra defensores de los derechos humanos, periodistas y otros trabajadores de los medios de comunicación, y tomen medidas específicas de protección contra las violaciones del derecho a la privacidad, entre otras cosas regulando la venta, la transferencia, el uso y la exportación de tecnologías de vigilancia;

o) Promuevan una educación de calidad, accesible e inclusiva y oportunidades de educación permanente para todos, a fin de fomentar, entre otras cosas, la alfabetización digital y las aptitudes técnicas necesarias para proteger eficazmente su privacidad, inclusive mediante formación sobre seguridad en línea, orientación y sensibilización, y garanticen la disponibilidad de formación adecuada para las partes interesadas pertinentes en este ámbito;

p) Se abstengan de exigir a las empresas que adopten medidas que interfieran con el derecho a la privacidad de forma arbitraria o ilegal y protejan a las personas frente a los daños, incluidos los causados por las empresas mediante la recopilación, el procesamiento, el almacenamiento y el intercambio de datos y la elaboración de perfiles, así como mediante el uso de procesos automatizados y el aprendizaje automático;

q) Intensifiquen los esfuerzos para combatir la discriminación resultante del uso de sistemas de inteligencia artificial, entre otras cosas ejerciendo la diligencia debida para evaluar, prevenir y mitigar las repercusiones negativas de su aplicación en los derechos humanos;

11. *Alienta* a todas las empresas, en particular a las empresas comerciales que recopilan, almacenan, utilizan, comparten y procesan datos, a que:

a) Examinen sus modelos de negocio y se aseguren de que sus procesos de diseño y desarrollo, sus operaciones comerciales y sus prácticas de recopilación y procesamiento de datos estén en consonancia con los Principios Rectores sobre las Empresas y los Derechos Humanos: Puesta en Práctica del Marco de las Naciones Unidas para “Proteger, Respetar y Remediar”, y pongan de relieve la importancia de llevar a cabo la diligencia debida en materia de derechos humanos con respecto a sus productos, en particular con respecto al papel de los algoritmos y los sistemas de clasificación;

b) Informen a los usuarios, de una manera clara, acorde a la edad y fácilmente accesible, incluso para las personas con discapacidad, sobre la recopilación, la utilización, el intercambio y la retención de sus datos que puedan afectar a su derecho a la privacidad y se abstengan de hacerlo sin su consentimiento o un fundamento jurídico, y establezcan un régimen de transparencia y políticas que permitan el consentimiento libre, informado y efectivo de los usuarios;

c) Integren el derecho a la privacidad y otros derechos humanos pertinentes en la elaboración de políticas internas, la ingeniería de productos, el desarrollo empresarial, la formación del personal y otros procesos internos relevantes;

d) Apliquen salvaguardias administrativas, técnicas y físicas para garantizar que los datos se procesen de manera lícita y que este procesamiento resulte necesario en función de sus fines, garanticen la legitimidad de tales fines y la precisión, integridad y confidencialidad del procesamiento, e impidan la divulgación o el uso de datos sin autorización;

e) Velen por que las personas tengan acceso a sus datos y por que puedan modificarlos, rectificarlos, actualizarlos, suprimirlos y retirar el consentimiento para su utilización, en particular si son incorrectos o inexactos, o si los datos se hubiesen obtenido de forma ilegal o utilizado a efectos discriminatorios;

f) Velen por que se incorpore el respeto del derecho a la privacidad y otros derechos humanos pertinentes en el diseño, funcionamiento, evaluación y regulación de la adopción automatizada de decisiones y las tecnologías de aprendizaje automático, y prevean recursos efectivos, incluidas indemnizaciones, por las transgresiones de los derechos humanos que hayan causado, a las que hayan contribuido o con las que se les vincule;

g) Establezcan salvaguardias adecuadas destinadas a prevenir o mitigar los efectos negativos en los derechos humanos que estén directamente relacionados con sus operaciones, productos o servicios, entre otras formas, cuando sea necesario, mediante cláusulas contractuales, e informen sin demora a los órganos de supervisión pertinentes, nacionales, regionales o internacionales, de las transgresiones o vulneraciones cuando detecten el uso indebido de sus productos y servicios;

h) Intensifiquen los esfuerzos para combatir la discriminación resultante del uso de sistemas de inteligencia artificial, entre otras cosas mediante la diligencia debida en materia de derechos humanos y la supervisión y evaluación de los sistemas de inteligencia artificial a lo largo de su ciclo vital, así como la repercusión de su aplicación en los derechos humanos;

i) Fomenten que la toma de decisiones algorítmicas, los sistemas automatizados y los sistemas que requieren participación humana sean transparentes y se puedan explicar adecuadamente, y garanticen que los datos utilizados para el entrenamiento de algoritmos sean representativos y se hayan recopilado legalmente;

j) Establezcan medidas de salvaguardia adecuadas para garantizar que la distribución y transferencia de datos dentro de las organizaciones y entre ellas y la reorganización de los datos, entre otros a través de computación en la nube, conjuntos de datos no estructurados, tecnología de cadenas de bloques, realidad aumentada e Internet de los objetos, sean compatibles con la protección de datos y el derecho a la privacidad;

k) Adopten las medidas adecuadas a lo largo del ciclo de vida de los sistemas de inteligencia artificial y las tecnologías digitales, incluso antes de iniciar el diseño y desarrollo de aplicaciones y programas informáticos que impliquen el tratamiento de datos personales, con vistas a establecer un sistema de supervisión y gestión de riesgos que garantice que los datos se tratan de forma justa y lícita;

12. *Alienta* a las empresas comerciales, incluidas las que proveen servicios de comunicaciones, a que procuren facilitar soluciones para asegurar y proteger la confidencialidad de las comunicaciones y transacciones digitales, como medidas de cifrado, uso de seudónimos y anonimato, y garanticen la aplicación de salvaguardias que respeten los derechos humanos, y exhorta a los Estados a fomentar medidas y soluciones técnicas que propicien prácticas robustas de cifrado, uso de seudónimos y anonimato, a no interferir en el uso de esas soluciones técnicas, a que cualquier restricción a las mismas se ajuste a las obligaciones que incumben a los Estados con arreglo al derecho internacional de los derechos humanos, y a que aprueben políticas que protejan la privacidad de las comunicaciones digitales de las personas;

13. *Alienta* a los Estados y, en su caso, a las empresas, a que lleven a cabo sistemáticamente la diligencia debida en materia de derechos humanos a lo largo del ciclo de vida de los sistemas de inteligencia artificial que conciban, diseñen, desarrollen, desplieguen, vendan, obtengan o exploten, incluida la realización de evaluaciones periódicas y exhaustivas de su efecto para los derechos humanos y la participación de todas las partes interesadas pertinentes;

14. *Alienta* a todas las partes interesadas a que incorporen una perspectiva de género en la conceptualización, el desarrollo y la aplicación de las tecnologías digitales y las políticas conexas y a que promuevan la participación de las mujeres para hacer frente a la violencia y la discriminación contra las mujeres y las niñas que tienen lugar mediante el uso de tecnologías o cuyo efecto se ve ampliado por él, entre otras cosas alentando a las empresas de tecnología digital, incluidos los proveedores de servicios de Internet, a respetar las normas y aplicar mecanismos de presentación de informes transparentes y accesibles;

15. *Solicita* a la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos que prepare 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, incluidas las cuestiones tratadas en la presente resolución, a fin de determinar y aclarar los principios de derechos humanos, las salvaguardias y las mejores prácticas conexos, y que presente el informe al Consejo de Derechos Humanos en su 57º período de sesiones, al que seguirá un diálogo interactivo;

16. *Solicita también* a la Oficina del Alto Comisionado que, al preparar el informe mencionado, recabe aportaciones de los interesados y tenga en cuenta la labor ya realizada por los interesados pertinentes de diversas regiones geográficas, incluidos los Estados, las organizaciones internacionales y regionales, los procedimientos especiales del Consejo de Derechos Humanos, los órganos creados en virtud de tratados, otras oficinas, organismos, fondos y programas pertinentes de las Naciones Unidas, en el marco de sus respectivos mandatos, las instituciones nacionales de derechos humanos, la sociedad civil, el sector privado, la comunidad técnica y las instituciones académicas.

48ª sesión
12 de octubre de 2023

[Aprobada sin votación.]