



Asamblea General

Distr. general
13 de octubre de 2021
Español
Original: inglés

Consejo de Derechos Humanos

48º período de sesiones

13 de septiembre a 11 de octubre de 2021

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 7 de Octubre de 2021

48/4. 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 aprobadas por la Asamblea General y el Consejo de Derechos Humanos relativas al derecho a la privacidad en la era digital y la reciente prórroga del mandato de la Relatora Especial sobre el derecho a la privacidad¹, 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 digital², haciendo notar con interés sus informes sobre la cuestión y recordando el seminario de expertos sobre el derecho a la privacidad en la era digital organizado por la Oficina del Alto Comisionado los días 27 y 28 de mayo de 2020, en el que se señaló el impacto cada vez mayor del uso de las tecnologías de inteligencia artificial en el ejercicio del derecho a la privacidad, se planteó inquietud por la transparencia en relación con la recopilación y el intercambio de datos personales subyacentes en algunas partes de los sistemas de inteligencia artificial y se expresó preocupación por las repercusiones negativas de la aplicación de la inteligencia artificial en la privacidad,

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 tomando nota de sus contribuciones a la promoción y protección del derecho a la privacidad,

Tomando nota de la Hoja de Ruta del Secretario General para la Cooperación Digital, presentada en junio de 2020,

¹ Resolución 46/16.

² Véase A/HRC/48/31.



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 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,

Afirma que los derechos de las personas también deben estar protegidos en Internet, incluido el derecho a la privacidad, y señalando que la sincronización acelerada de los espacios de Internet y de otros ámbitos puede afectar a las personas, incluido su derecho a la privacidad,

Observando que los procesos de toma de decisiones algorítmicas o automatizadas en Internet 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,

Observando además que las mujeres y las niñas experimentan violaciones y abusos de su derecho a la privacidad por motivos de género, tanto en Internet como en otros ámbitos, así como violaciones o abusos que tienen repercusiones en función del género,

Reconociendo que la promoción, la protección y el respeto del derecho a la privacidad son importantes para prevenir la violencia, incluida la violencia sexual y de género, el abuso y el acoso sexual, en particular contra mujeres, niñas y niños y personas con discapacidad, así como cualquier forma de discriminación, que puede tener lugar en espacios digitales y en línea e incluye la ciberintimidación y el ciberacoso,

Reconociendo que los derechos humanos deben tenerse en cuenta en la concepción, el diseño, la utilización, el despliegue y el ulterior desarrollo de tecnologías nuevas y emergentes, como las que entrañan el uso de inteligencia artificial, ya que pueden, sin las salvaguardias adecuadas, afectar al 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 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 la inteligencia artificial que requiere 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, puede entrañar graves riesgos para el derecho a la privacidad, en particular cuando se emplea para la identificación, la verificación, el rastreo, la elaboración de perfiles, el reconocimiento facial, la predicción de la conducta o la aplicación de sistemas de puntuación de las personas,

Poniendo de relieve que la preocupación por la privacidad no debe desecharse por considerarse una barrera a la innovación,

Observando que la utilización de la extracción de datos y los 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,

Observando también la preocupación pública respecto de 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 que ciertos algoritmos predictivos pueden dar lugar a discriminación cuando se utilizan datos no representativos,

Reconociendo que deben evitarse los resultados discriminatorios por motivos raciales o de otro tipo en la concepción, el diseño, el desarrollo, el despliegue y el uso de las tecnologías digitales nuevas y emergentes,

Observando con preocupación que los informes indican una menor precisión de las tecnologías de reconocimiento facial en relación con determinados grupos, en particular las personas no blancas y las mujeres, entre otras cosas cuando se usan datos de formación no representativos, que la utilización de las tecnologías digitales puede reproducir, reforzar e incluso exacerbar la desigualdad racial, y que en este contexto los recursos efectivos revisten importancia,

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,

Reconociendo la necesidad de garantizar el respeto del derecho internacional de los derechos humanos en la concepción, el diseño, el desarrollo, el despliegue, la evaluación y la regulación de las tecnologías basadas en datos y de garantizar que estén sujetas a las salvaguardias y la supervisión adecuadas,

Expresando preocupación porque con frecuencia las personas no dan o no pueden dar su consentimiento libre, explícito e informado a la recopilación, el procesamiento y el almacenamiento de sus datos o a los efectos de la reutilización, la venta o la reventa múltiple de sus datos personales, ya que en la era digital han aumentado considerablemente la recopilación, el procesamiento, el uso, el almacenamiento y el intercambio de datos personales, incluidos datos delicados,

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 ninguna injerencia en el derecho a la privacidad debe ser arbitraria o ilegal, 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, *Poniendo de relieve* que la vigilancia o la interceptación ilegales o arbitrarias de las comunicaciones, la recopilación ilegal o arbitraria de datos personales o la piratería informática ilegal o arbitraria y la utilización ilegal o arbitraria de tecnologías biométricas, al constituir actos sumamente intrusivos, violan o vulneran el derecho a la privacidad y pueden interferir con otros derechos humanos, incluido el derecho a la libertad de expresión y a abrigar opiniones sin injerencias, y el derecho a la libertad de reunión y asociación

pacíficas, y pueden ser contrarias a los preceptos de una sociedad democrática, en particular cuando se llevan a cabo extraterritorialmente o a gran escala,

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 pueden sufrir con frecuencia amenazas, acoso e inseguridad, así como injerencias ilegales o arbitrarias en su derecho a la privacidad, como resultado de sus actividades,

Observando con profunda preocupación también el uso de herramientas tecnológicas desarrolladas por la industria de la vigilancia privada por parte de agentes privados o públicos para llevar a cabo la vigilancia, la piratería de dispositivos y sistemas, la interceptación y la interrupción de las comunicaciones, así como la recopilación de datos, interfiriendo en la vida profesional y privada de las personas, incluidas las que promueven y defienden los derechos humanos y las libertades fundamentales, los periodistas y otros trabajadores de los medios de difusión, en violación o abuso de sus derechos humanos, específicamente el derecho a la privacidad,

Recordando que las empresas comerciales 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 de las Naciones Unidas para los Derechos Humanos sobre la aplicación de estos principios sobre 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, en particular las medidas de cifrado, uso de seudónimos y anonimato, a fin de garantizar el disfrute de los derechos humanos, incluidos los derechos a la privacidad, la libertad de opinión y de expresión y la libertad de reunión y de asociación pacíficas,

Observando la importancia de proteger y respetar el derecho de las personas a la privacidad al diseñar, desarrollar o desplegar medios tecnológicos en respuesta a desastres, epidemias y pandemias, especialmente a la pandemia de enfermedad por coronavirus (COVID-19), como la notificación digital de la exposición y el rastreo de contactos,

Observando también que las tecnologías digitales nuevas y emergentes pueden contribuir a la lucha contra la pandemia de COVID-19, y recordando a este respecto la importancia de proteger los datos relacionados con la salud, y observando con preocupación que algunas iniciativas para combatir la pandemia de COVID-19 tienen repercusiones negativas en el disfrute del derecho a la privacidad,

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 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 y emocional, tienen cuando no cuentan con las salvaguardias debidas en el disfrute del derecho a la privacidad y 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;

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. *Reconoce* que los riesgos para el derecho a la privacidad y otros derechos humanos pueden y deben reducirse al mínimo mediante la adopción de una normativa

adecuada o de otros mecanismos apropiados, de conformidad con las obligaciones aplicables en virtud del derecho internacional de los derechos humanos para la concepción, el diseño, el desarrollo y el despliegue de las 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;

6. *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 impedir las, como cerciorarse de que la legislación nacional pertinente se ajusta a sus obligaciones en virtud del derecho internacional de los derechos humanos;

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) 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;

e) 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;

f) 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 mediante la recopilación, el procesamiento, la retención o la utilización ilegales o arbitrarios de datos personales por particulares, Gobiernos, empresas y organizaciones privadas;

g) Consideren la posibilidad de aprobar o revisar leyes, reglamentos o políticas para asegurarse de que las empresas incorporan plenamente el derecho a la privacidad y otros derechos humanos pertinentes cuando conciben, desarrollen, desplieguen y evalúen tecnologías, incluida la inteligencia artificial, 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;

h) Sigam 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;

i) Elaboren, examinen, apliquen y fortalezcan políticas con perspectiva de género que promuevan y protejan el derecho de todas las personas a la privacidad en la era digital;

j) 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;

k) Se abstengan de utilizar las tecnologías de vigilancia de una manera que no cumpla con las obligaciones internacionales en materia de derechos humanos, también

cuando se utilizan contra periodistas y defensores de los derechos humanos, 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;

l) Promuevan una educación de calidad 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;

m) Garanticen la disponibilidad de formación pertinente para jueces, abogados, fiscales y otros profesionales relevantes del sistema judicial sobre el funcionamiento de las tecnologías digitales nuevas y emergentes y su impacto en los derechos humanos;

n) 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;

o) 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 privada de los usuarios;

p) Elaboren o mantengan legislación, medidas preventivas y recursos para hacer frente a los daños causados por el procesamiento, la utilización, la venta o la reventa múltiple u otros intercambios mercantiles de datos personales sin el consentimiento libre, explícito e informado de los interesados;

q) Adopten medidas adecuadas para garantizar que los programas de identidad digital o biométrica se conciban, apliquen y ejecuten con las debidas salvaguardias jurídicas y técnicas en vigor y con pleno cumplimiento del derecho internacional de los derechos humanos;

r) 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;

7. *Alienta* a todos los Estados a que promuevan un entorno de tecnología de la información y las comunicaciones abierto, seguro, estable, accesible y pacífico, basado en el respeto del derecho internacional, incluidas las obligaciones consagradas en la Carta de las Naciones Unidas y los instrumentos internacionales de derechos humanos;

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

a) Cumplan su obligación de respetar los derechos humanos, de conformidad 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”, incluido el derecho a la privacidad en la era digital, e intensifiquen sus esfuerzos en este sentido;

b) Informen a los usuarios 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 informado de los usuarios;

c) 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, y garanticen la legitimidad de esos fines y la precisión, integridad y confidencialidad del procesamiento;

d) Velen por que las personas tengan acceso a sus datos y por que puedan modificarlos, rectificarlos, actualizarlos y suprimirlos, en particular si son incorrectos o inexactos, o si los datos se hubiesen obtenido de forma ilegal;

e) 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 o a las que hayan contribuido;

f) 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;

g) 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;

9. *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 no interferir en el uso de esas soluciones técnicas, y 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;

10. *Alienta* a los Estados y, en su caso, a las empresas comerciales a que ejerzan la diligencia debida en materia de derechos humanos a lo largo del ciclo vital de los sistemas de inteligencia artificial que diseñen, desarrollen, desplieguen o vendan u obtengan y exploten;

11. *Solicita* a la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos que prepare un informe escrito en el que se describan las tendencias y los problemas recientes en relación con el derecho humano a la privacidad, 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 conexas, y que presente el informe al Consejo de Derechos Humanos en su 51º período de sesiones, seguido de un diálogo interactivo;

12. *Solicita* a la Oficina del Alto Comisionado que, al preparar el informe mencionado, recabe aportaciones de los interesados y tenga en cuenta la labor pertinente ya realizada por los interesados 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.

41ª sesión
7 de octubre de 2021

[Aprobada sin votación.]