Naciones Unidas A/RES/79/175

Asamblea General

Distr. general
19 de diciembre de 2024

**Septuagésimo noveno período de sesiones**
Tema 71 b) del programa
**Promoción y protección de los derechos humanos: cuestiones de derechos humanos, incluidos otros medios de mejorar el goce efectivo de los derechos humanos y las libertades fundamentales**

# Resolución aprobada por la Asamblea General el 17 de diciembre de 2024

[*sobre la base del informe de la Tercera Comisión (A/79/458/Add.2, párr. 99)*]

## 79/175. El derecho a la privacidad en la era digital

*La Asamblea General*,

*Reafirmando* los propósitos y principios de la Carta de las Naciones Unidas, los derechos humanos y las libertades fundamentales consagrados en la Declaración Universal de Derechos Humanos[1] y los tratados internacionales de derechos humanos pertinentes, incluidos el Pacto Internacional de Derechos Civiles y Políticos[2] y el Pacto Internacional de Derechos Económicos, Sociales y Culturales[3], así como la Declaración y Programa de Acción de Viena[4],

*Recordando* sus resoluciones 68/167, de 18 de diciembre de 2013, 69/166, de 18 diciembre de 2014, 71/199, de 19 de diciembre de 2016, 73/179, de 17 de diciembre de 2018, 75/176, de 16 de diciembre de 2020, y 77/211, de 15 de diciembre de 2022, relativas al derecho a la privacidad en la era digital, y la resolución 45/95, de 14 de diciembre de 1990, relativa a los principios rectores sobre la reglamentación de los ficheros computarizados de datos personales, así como las resoluciones del Consejo de Derechos Humanos 28/16, de 26 de marzo de 2015[5], 34/7, de 23 de marzo de 2017[6], 37/2 de 22 de marzo de 2018[7], 42/15, de 26 de septiembre de 2019[8], 48/4, de

[1] Resolución 217 A (III).
[2] Véase la resolución 2200 A (XXI), anexo.
[3] *Ibid.*
[4] A/CONF.157/24 (Part I), cap. III.
[5] Véase *Documentos Oficiales de la Asamblea General, septuagésimo período de sesiones, suplemento núm. 53* (A/70/53), cap. III, secc. A.
[6] *Ibid., septuagésimo segundo período de sesiones, suplemento núm. 53* (A/72/53), cap. IV, secc. A.
[7] *Ibid., septuagésimo tercer período de sesiones, suplemento núm. 53* (A/73/53), cap. IV, secc. A.
[8] *Ibid., septuagésimo cuarto período de sesiones, suplemento núm. 53A* (A/74/53/Add.1), cap. III.



Se ruega reciclar

7 de octubre de 2021[9], y 54/21, de 16 de octubre de 2023[10], relativas al derecho a la privacidad en la era digital, y las resoluciones 32/13, de 1 de julio de 2016[11], 38/7, de 5 de julio de 2018[12], 47/16, de 13 de julio de 2021[13], y 57/29, de 11 de octubre de 2024[14], relativas a la promoción, protección y disfrute de los derechos humanos en Internet,

*Recordando también* el documento final de la reunión de alto nivel de la Asamblea General sobre el examen general de la aplicación de los resultados de la Cumbre Mundial sobre la Sociedad de la Información[15],

*Tomando nota* de los informes del anterior Relator Especial y de la Relatora Especial sobre el derecho a la privacidad[16], los informes del anterior Relator Especial y de la Relatora Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión[17] y los informes pertinentes del Relator Especial sobre los derechos a la libertad de reunión pacífica y de asociación[18], así como de la Relatora Especial sobre las formas contemporáneas de racismo, discriminación racial, xenofobia y formas conexas de intolerancia[19],

*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, haciendo notar con interés los informes del Alto Comisionado sobre la cuestión[20], y recordando los talleres de expertos sobre el derecho a la privacidad en la era digital, celebrados los días 19 y 20 de febrero de 2018 y 27 y 28 de mayo de 2020,

*Tomando nota* de las iniciativas del Secretario General sobre las nuevas tecnologías, como el Llamamiento a la Acción en favor de los Derechos Humanos, puesto en marcha en 2020, la hoja de ruta para la cooperación digital, presentada en junio de 2020, los Principios Globales de las Naciones Unidas para la Integridad de la Información, el establecimiento en mayo de 2024 de las directrices sobre la diligencia debida en materia de derechos humanos para el uso de la tecnología digital y la creación de la Oficina del Enviado del Secretario General para la Tecnología, y observando los debates que se celebran cada año en el Foro para la Gobernanza de Internet, que es un foro de múltiples partes interesadas para debatir cuestiones de gobernanza de Internet y cuyo mandato fue prorrogado en 2015 por la Asamblea General por otros diez años, y reconociendo que para enfrentar con eficacia los desafíos relacionados con el derecho a la privacidad en el contexto de la tecnología moderna de las comunicaciones se requiere una cooperación constante y concertada de múltiples partes interesadas,

*Acogiendo con* beneplácito la celebración de la Cumbre del Futuro, que tuvo lugar los días 22 y 23 de septiembre de 2024 en la Sede de las Naciones Unidas (Nueva York), y reiterando la necesidad de prestar a los países en desarrollo un apoyo

[9] *Ibid., septuagésimo sexto período de sesiones, suplemento núm. 53A* (A/76/53/Add.1), cap. IV, secc. A.
[10] *Ibid., septuagésimo octavo período de sesiones, suplemento núm. 53A* (A/78/53/Add.1), cap. III, secc. A.
[11] *Ibid., septuagésimo primer período de sesiones, suplemento núm. 53* (A/71/53), cap. V, secc. A.
[12] *Ibid., septuagésimo tercer período de sesiones, suplemento núm. 53* (A/73/53), cap. VI, secc. A.
[13] *Ibid., septuagésimo sexto período de sesiones, suplemento núm. 53* (A/76/53), cap. VII, secc. A.
[14] *Ibid., septuagésimo noveno período de sesiones, suplemento núm. 53A* (A/79/53/Add.1), cap. III, secc. A.
[15] Resolución 70/125.
[16] A/HRC/43/52, A/HRC/46/37, A/HRC/49/55, A/HRC/52/37, A/HRC/55/46, A/75/147, A/76/220, A/77/196, A/78/310 y A/79/193.
[17] A/HRC/44/49, A/HRC/50/29, A/HRC/53/25, A/HRC/56/53, A/75/261, A/76/258 y A/78/288.
[18] A/HRC/44/50, A/HRC/50/23, A/HRC/50/42 y A/75/184.
[19] A/HRC/44/57, A/75/329 y A/76/434.
[20] A/HRC/48/31 y A/HRC/51/17.

adecuado que los ayude a aplicar las medidas del Pacto para el Futuro[21], incluido el Pacto Digital Global[22], que son pertinentes para el derecho a la privacidad y para colmar las brechas digitales en los países y entre ellos,

*Recordando* que, en línea 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"[23], la responsabilidad de respetar los derechos humanos exige que las empresas eviten que sus propias actividades provoquen o contribuyan a provocar consecuencias negativas sobre los derechos humanos y hagan frente a esas consecuencias cuando se produzcan, y traten de prevenir o mitigar las consecuencias negativas sobre los derechos humanos directamente relacionadas con operaciones, productos o servicios prestados por sus relaciones comerciales, incluso cuando no hayan contribuido a generarlos,

*Observando* que el rápido ritmo del desarrollo tecnológico permite a las personas de todo el mundo utilizar nuevas tecnologías de la información y las comunicaciones que empoderan a la gente, mejoran las vidas, fortalecen la justicia y aumentan la productividad, y, al mismo tiempo, incrementa la capacidad de los Gobiernos, las empresas y las personas de llevar a cabo actividades de vigilancia, interceptación y recopilación de datos, lo que podría constituir una violación o una transgresión de los derechos humanos, en particular del derecho a la privacidad, establecido en el artículo 12 de la Declaración Universal de Derechos Humanos y el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, 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, sobre todo en las niñas, las personas con discapacidad y las personas de edad, así como las personas en situaciones de vulnerabilidad,

*Reconociendo* que las tecnologías digitales nuevas y emergentes, en particular las tecnologías digitales de apoyo, pueden contribuir especialmente al pleno disfrute de los derechos humanos por parte de las personas con discapacidad, y que esas tecnologías deben diseñarse en consulta con ellas y con las salvaguardias adecuadas para proteger sus derechos, incluido el derecho a la privacidad,

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

*Observando* que las mujeres y las niñas experimentan violaciones y transgresiones específicas de su derecho a la privacidad, 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 y discursos de odio, lo que puede exacerbar los estereotipos de género y dar lugar a diversas formas de violencia, incluida la violencia de género, y expresando preocupación por la continuidad y la interrelación entre la violencia, el acoso y la discriminación contra las mujeres y las niñas en línea y en otros ámbitos, y

[21] Resolución 79/1.
[22] *Ibid.*, anexo I.
[23] A/HRC/17/31, anexo.

condenando el aumento de estos actos cometidos, asistidos, agravados o amplificados por el uso de la tecnología,

*Observando también* que los niños pueden ser particularmente vulnerables a las transgresiones y violaciones de su derecho a la privacidad,

*Observando además* que los Estados partes deben aplicar la Convención sobre los Derechos del Niño[24] en relación con el entorno digital, incluida la importancia de la privacidad para la capacidad de los niños de actuar por sí mismos, su dignidad y su seguridad, y para el ejercicio de sus derechos,

*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 esas injerencias, y reconociendo que el ejercicio del derecho a la privacidad es importante para materializar 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,

*Recordando con aprecio* la observación general núm. 16 del Comité de Derechos Humanos sobre el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos relativo al derecho a la privacidad, la familia, el domicilio y la correspondencia, y la protección de la honra y reputación[25], y observando también los grandes cambios tecnológicos que se han producido desde su aprobación, así como la necesidad de examinar el derecho a la privacidad habida cuenta de los problemas que se plantean en la era digital,

*Reconociendo* la necesidad de seguir examinando 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 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,

*Reconociendo también* que el examen del derecho a la privacidad debe basarse en las obligaciones internacionales y nacionales vigentes, incluido el derecho internacional de los derechos humanos, así como en los compromisos pertinentes, y no debe abrir el camino a injerencias indebidas en los derechos humanos de las personas,

*Reconociendo además* la necesidad de garantizar que se respeten las obligaciones internacionales en materia de 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,

*Destacando* la importancia del pleno respeto de la libertad de buscar, recibir y difundir información, incluida la importancia fundamental del acceso a la información y la participación democrática,

*Reconociendo* que el derecho a la privacidad es importante para el disfrute de otros derechos y puede contribuir a la capacidad de las personas de participar en la vida política, económica, social y cultural, y observando con preocupación que las violaciones o abusos del derecho a no sufrir injerencias ilícitas o arbitrarias en el

[24] Naciones Unidas, *Treaty Series*, vol. 1577, núm. 27531.

[25] *Documentos Oficiales de la Asamblea General, cuadragésimo tercer período de sesiones, suplemento núm. 40* (A/43/40), anexo VI.

derecho a la privacidad pueden afectar al disfrute de otros derechos humanos, en particular el derecho a la libertad de expresión y a abrigar opiniones sin injerencias y el derecho a la libertad de reunión pacífica y la libertad de asociación,

*Observando* 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, las relaciones sociales, las preferencias privadas y la identidad de una persona,

*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 a la reutilización, la venta o la reventa múltiple de sus datos personales, y que la recopilación, el procesamiento, el uso, el almacenamiento y el intercambio de datos personales, incluidos datos delicados, han aumentado considerablemente en la era digital,

*Observando* que en la observación general núm. 16 del Comité de Derechos Humanos se recomienda que los Estados tomen medidas eficaces para impedir la retención, el procesamiento y el uso ilegales de datos personales almacenados por las autoridades públicas y las empresas,

*Observando también* que el uso de la inteligencia artificial puede contribuir a promover y proteger los derechos humanos y puede llegar a transformar los Gobiernos y las sociedades, los sectores económicos y el mundo del trabajo, y que también puede tener diversas repercusiones de gran alcance, incluso con respecto al derecho a la privacidad,

*Observando además* que atenerse a los principios de transparencia, explicabilidad y, si procede, consentimiento efectivo de los usuarios al procesar datos personales utilizando la inteligencia artificial no solo ayuda a generar confianza y fiabilidad en las tecnologías de inteligencia artificial, sino que también contribuye a proteger los derechos humanos, por ejemplo permitiendo que se informe de manera oportuna, completa, sencilla y clara a las personas afectadas por esas tecnologías sobre aspectos básicos respecto al uso de su información personal en procesos o proyectos de inteligencia artificial y sus consecuencias, y sobre los motivos concretos que justifican ese uso,

*Observando con preocupación* que la brecha en materia de inteligencia artificial y otras brechas digitales entre los países y dentro de ellos siguen ampliándose, y que los países en desarrollo se enfrentan a desafíos singulares para seguir el ritmo de la rápida aceleración del desarrollo de la inteligencia artificial, en particular en lo que se refiere al diseño, desarrollo, despliegue y uso de la inteligencia artificial,

*Observando con preocupación también* que el uso de la inteligencia artificial o las tecnologías de aprendizaje automático, por ejemplo para herramientas de identificación biométrica a distancia, tecnología de reconocimiento facial o moderación automatizada de contenidos, puede, sin las debidas salvaguardias técnicas, reglamentarias, jurídicas y éticas, dar lugar a decisiones que podrían afectar al disfrute de los derechos humanos, incluidos los derechos económicos, sociales y culturales, y menoscabar la no discriminación, y reconociendo la necesidad de aplicar el derecho internacional de los derechos humanos y los marcos de protección de los datos al diseño, la evaluación y la reglamentación de esas prácticas,

*Reconociendo* que el uso de la inteligencia artificial, si bien puede tener importantes efectos positivos en los ámbitos económico y social, requiere y permite procesar grandes cantidades de datos, a menudo relacionados con información personal, incluidos datos biométricos y datos sobre el comportamiento, las relaciones

sociales, la raza o el origen étnico, la religión o las creencias de una persona, lo que puede plantear graves riesgos para el disfrute del derecho a la privacidad, sobre todo cuando se hace sin las debidas salvaguardias, en particular cuando se emplea para la identificación, el rastreo, la elaboración de perfiles, el reconocimiento facial, la clasificación, la predicción del comportamiento o la aplicación de sistemas de puntuación de las personas,

*Observando* que el uso de la inteligencia artificial, sin las debidas salvaguardias técnicas, reglamentarias, jurídicas y éticas puede plantear el riesgo de reforzar la discriminación, incluidas las desigualdades estructurales, y reconociendo que en la concepción, el desarrollo, la aplicación y el uso de las nuevas tecnologías digitales deben evitarse los resultados discriminatorios desde el punto de vista racial o desde cualquier otro punto de vista,

*Reconociendo* que el diseño, el desarrollo, la implantación y el uso incorrectos o maliciosos de los sistemas de inteligencia artificial, por ejemplo sin salvaguardias adecuadas o de manera contraria al derecho internacional, plantean riesgos que podrían dificultar los avances hacia la consecución de la Agenda 2030 para el Desarrollo Sostenible[26] y sus Objetivos de Desarrollo Sostenible y socavar el desarrollo sostenible en sus tres dimensiones —económica, social y ambiental—, agrandar las brechas digitales entre los países y dentro de ellos, reforzar las desigualdades y los sesgos estructurales, conducir a la discriminación, minar la integridad de la información y el acceso a ella, y debilitar la protección, la promoción y el goce de los derechos humanos y las libertades fundamentales, incluido el derecho a no sufrir injerencias ilícitas o arbitrarias en la vida privada,

*Observando con preocupación* que ciertos algoritmos de predicción pueden ocasionar discriminación, incluso cuando se utilizan datos no representativos,

*Observando* que el uso de procesos de adopción de decisiones algorítmicos o automatizados en línea puede afectar el disfrute de los derechos de las personas fuera de línea,

*Observando también* que el uso de la extracción de datos y de algoritmos para orientar los contenidos hacia los usuarios en línea puede socavar la integridad de la información, la capacidad de los usuarios de actuar por sí mismos y acceder a la información en línea, así como el derecho a la privacidad, lo cual puede propiciar que se intensifiquen las amenazas de la información errónea, la desinformación y el discurso de odio, y desembocar en 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[27],

*Observando con preocupación* que los informes indican una menor precisión de las tecnologías de reconocimiento facial con determinados grupos, incluso cuando se utilizan datos de entrenamiento no representativos, que el uso de las tecnologías digitales puede exacerbar la desigualdad racial y, en este contexto, la importancia de contar con recursos efectivos,

*Poniendo de relieve* que la vigilancia y la interceptación ilegales o arbitrarias de las comunicaciones, así como la recopilación ilegal o arbitraria de datos personales, la piratería informática y el uso ilícito de las tecnologías biométricas, al constituir actos de intrusión grave, violan el derecho a la privacidad y pueden interferir con el derecho a la libertad de expresión y a abrigar opiniones sin injerencias, el derecho a la libertad de reunión y de asociación pacíficas, y el derecho a la libertad de religión

[26] Resolución 70/1.
[27] A/HRC/22/17/Add.4, apéndice.

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

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

*Observando* que la sincronización acelerada de los espacios en línea y fuera de línea puede afectar al disfrute de los derechos humanos, incluido el derecho a la intimidad,

*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,

*Expresando preocupación* por la difusión de información errónea y desinformación, en particular en las plataformas de medios sociales, que se pueden concebir e implementar de manera que induzcan a error, difundan el racismo, la xenofobia, los estereotipos negativos y la estigmatización, violen y conculquen los derechos humanos, incluido el derecho a la privacidad, frenen la libertad de expresión, incluida la libertad de buscar, recibir y difundir información, e inciten a todas las formas de violencia, odio, intolerancia, discriminación y hostilidad, y poniendo de relieve la importante contribución de los periodistas, la sociedad civil y los círculos académicos a la labor para contrarrestar esta tendencia,

*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 y por actores privados o públicos para llevar a cabo la vigilancia, la piratería de dispositivos y sistemas, 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 abuso de sus derechos humanos, específicamente del derecho a la privacidad,

*Poniendo de relieve* que los Estados deben respetar las obligaciones internacionales en materia de derechos humanos en lo referente al derecho a la privacidad cuando intercepten las comunicaciones digitales de las personas o reúnan datos personales, cuando compartan los datos reunidos, entre otras cosas, mediante acuerdos de intercambio de información e inteligencia o den acceso a esos datos por otros medios, y cuando exijan a terceros, incluidas las empresas, la divulgación de datos personales,

*Observando* el aumento de la reunión de información biométrica sensible de las personas, y destacando que los Estados deben cumplir sus obligaciones en materia de derechos humanos y que las empresas deben respetar el derecho a la privacidad y otros derechos humanos cuando recopilen, procesen, compartan y almacenen

información biométrica, entre otras cosas adoptando políticas de protección de datos y salvaguardias,

*Profundamente preocupada* por los efectos negativos que pueden tener para el ejercicio y el goce de los derechos humanos la vigilancia y la interceptación de las comunicaciones, incluidas la vigilancia y la interceptación extraterritoriales de las comunicaciones y la recopilación de datos personales, en particular cuando se llevan a cabo a gran escala,

*Poniendo de relieve* que, en la era digital, es importante contar con soluciones técnicas para asegurar y proteger la confidencialidad de las comunicaciones y transacciones digitales, incluidas 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 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,

*Observando* que, aun cuando las consideraciones relacionadas con la seguridad pública pueden justificar la reunión y la protección de determinada información delicada, los Estados deben garantizar el pleno cumplimiento de sus obligaciones de conformidad con el derecho internacional de los derechos humanos,

*Observando también*, a ese respecto, que la prevención y represión del terrorismo redundan en el interés público y tienen gran importancia, y reafirmando a la vez que los Estados deben cerciorarse de que toda medida que se adopte para luchar contra el terrorismo sea conforme con sus obligaciones con arreglo al derecho internacional, en particular el derecho internacional de los derechos humanos, el derecho internacional de los refugiados y el derecho internacional humanitario,

*Reconociendo* que la falta de acceso a tecnologías y servicios asequibles y fiables sigue siendo un problema fundamental para muchos países en desarrollo,

*Destacando* la necesidad de abordar los desafíos existentes para salvar las brechas digitales, entre los países y dentro de ellos, y la brecha digital de género, y de aprovechar las tecnologías de la información y las comunicaciones para el desarrollo, y recordando la necesidad de hacer hincapié en la calidad del acceso para salvar las brechas digitales y de conocimientos, aplicando un enfoque multidimensional que incluya la velocidad, la estabilidad, la asequibilidad, el idioma, la capacitación, el fomento de la capacidad, el contenido local y la accesibilidad para las personas con discapacidad, y de promover el disfrute pleno de los derechos humanos, incluido el derecho a la privacidad,

*Destacando también* la necesidad de garantizar que las medidas de seguridad nacional y 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, 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, y los datos personales en la respuesta a emergencias sanitarias o de otro tipo,

*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, y recordando a este respecto la importancia de proteger los datos relacionados con la salud y otros datos personales, observando también que las nuevas tecnologías digitales emergentes pueden contribuir a la recuperación de las emergencias sanitarias mundiales,

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. *Reconoce* la naturaleza global y abierta de Internet y el rápido avance de las tecnologías de la información y las comunicaciones como fuerza que acelera los progresos hacia el desarrollo en sus distintas formas, incluso el logro de los Objetivos de Desarrollo Sostenible;

3. *Afirma* que los derechos que las personas tienen fuera del entorno virtual también deben estar protegidos en este, incluido el derecho a la privacidad, prestando especial atención a la protección de las niñas y los niños;

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

5. *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 de derechos humanos;

6. *Reconoce* que la concepción, el diseño, el uso, el despliegue y el desarrollo ulterior de tecnologías nuevas y emergentes, como las que utilizan inteligencia artificial, pueden repercutir en el disfrute del derecho a la privacidad y otros derechos humanos, y que los riesgos que se plantean a esos derechos pueden y deben evitarse o reducirse al mínimo adoptando reglamentos adecuados u otros mecanismos pertinentes o adaptando los que existan, de conformidad con las obligaciones aplicables con arreglo al derecho internacional de los derechos humanos, para la concepción, el diseño, el desarrollo y el despliegue de tecnologías nuevas y emergentes, incluida la inteligencia artificial, adoptando medidas para garantizar que exista una infraestructura de datos de calidad segura, transparente y responsable, y desarrollando mecanismos de auditoría y reparación basados en los derechos humanos y estableciendo una supervisión humana;

7. *Destaca* que los sistemas de vigilancia biométrica a distancia, incluidos los de reconocimiento facial, cuando se utilizan sin las salvaguardias adecuadas y específicas, suscitan gran preocupación en cuanto a su proporcionalidad, dado su carácter altamente invasivo y sus amplias repercusiones en un gran número de personas;

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

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

b) Inviten a todas las partes interesadas a seguir debatiendo cómo los fenómenos emergentes, como el impulso de la aprobación generalizada de las tecnologías de cadena de bloques, realidad expandida y virtual y el desarrollo de una neurotecnología cada vez más potente, sin las debidas salvaguardias, afectan el disfrute del derecho a la intimidad y el derecho a la libertad de opinión y expresión;

c) Adopten medidas para poner fin a las violaciones del derecho a la privacidad y creen las condiciones necesarias para impedirlas, como cerciorarse de que la legislación nacional pertinente se ajuste a sus obligaciones en virtud del derecho internacional de los derechos humanos;

d) Examinen periódicamente sus procedimientos, prácticas y legislación en relación con la vigilancia y la interceptación de las comunicaciones y la recopilación de datos personales, incluidas la vigilancia, interceptación y recopilación a gran escala, así como en relación con el uso de tecnologías de elaboración de perfiles, adopción automatizada de decisiones, aprendizaje automático y biometría, con miras a afianzar el derecho a la privacidad, velando por que se dé cumplimiento pleno y efectivo a todas sus obligaciones en virtud del derecho internacional de los derechos humanos;

e) Establezcan o mantengan mecanismos nacionales de supervisión, de índole judicial, administrativa o parlamentaria, que cuenten con los recursos necesarios y sean independientes, efectivos e imparciales, así como capaces de asegurar la transparencia, cuando proceda, y la rendición de cuentas por las actividades de vigilancia de las comunicaciones, su interceptación y la recopilación de datos personales que realice el Estado;

f) Proporcionen acceso a un recurso efectivo a las personas cuyo derecho a la privacidad haya sido violado mediante la vigilancia ilegal o arbitraria, de conformidad con las obligaciones internacionales en materia de derechos humanos;

g) Examinen la posibilidad de elaborar o mantener y aplicar una legislación adecuada, en consulta con todos los interesados pertinentes, incluidas las empresas, las organizaciones internacionales y la sociedad civil, con sanciones eficaces y vías de recurso adecuadas, que proteja a las personas contra las violaciones y las transgresiones del derecho a la privacidad, concretamente la recopilación, el procesamiento, la retención, el intercambio o el uso ilegales y arbitrarios de datos personales por particulares, Gobiernos, empresas y organizaciones privadas;

h) Consideren la posibilidad de elaborar o mantener y aplicar leyes, reglamentos y políticas para asegurarse de que todas las empresas, incluidas las de medios sociales y otras plataformas en línea, respeten 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 indemnización y garantías de no repetición;

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 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 los abusos y recibir comunicaciones de particulares y organizaciones, y ofrecer vías de recurso adecuadas;

j) 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, incluidas, con repercusiones particulares, las mujeres, así como los niños;

k) Consideren la posibilidad de elaborar, examinar, aplicar y fortalecer políticas y programas con perspectiva de género que contribuyan al empoderamiento de todas las mujeres y las niñas y que promuevan y protejan el derecho de todas las personas a la privacidad en la era digital;

l) 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;

m) Promuevan una educación de calidad y oportunidades de educación permanente para todos a fin de fomentar, entre otras cosas, los conocimientos digitales y las aptitudes técnicas necesarias para proteger eficazmente la privacidad;

n) Se abstengan de exigir a las empresas que adopten medidas que interfieran con el derecho a la privacidad de manera arbitraria o ilegal;

o) Protejan a las personas de las violaciones o transgresiones del derecho a la privacidad, incluidas las causadas por la reunión, el procesamiento, el almacenamiento y el intercambio arbitrarios o ilegales de datos, la elaboración de perfiles y la utilización de procesos automatizados y el aprendizaje automático;

p) Faciliten que las empresas puedan adoptar las medidas voluntarias de transparencia adecuadas en relación con las solicitudes de las autoridades estatales que requieren acceso a datos e información privada de los usuarios;

q) Consideren la posibilidad de elaborar o mantener legislación, medidas preventivas y recursos ante los daños derivados del procesamiento, el uso, la venta, la reventa múltiple u otros intercambios mercantiles de datos personales sin el consentimiento libre, explícito efectivo e informado de los interesados;

r) 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;

s) Velen por que las autoridades independientes establecidas a nivel nacional que se ocupan de la protección de datos incorporen los debidos mecanismos de vigilancia;

9. *Exhorta* a todas las empresas, en particular aquellas que reúnen, 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 y adecuada a la edad que resulte fácilmente accesible, incluso para las personas con discapacidad, sobre la recopilación, el uso, el intercambio y la retención de los datos que puedan afectar su derecho a la privacidad, se abstengan de hacerlo sin su consentimiento ni base legal, y establezcan y ejecuten políticas de transparencia que permitan el consentimiento libre, informado y efectivo de los usuarios, según proceda;

c) Apliquen salvaguardias administrativas, técnicas y físicas para garantizar que los datos se procesen de manera lícita y que este procesamiento se limite a lo necesario en relación con sus fines, y que se aseguren la legitimidad de estos fines y la precisión, integridad y confidencialidad del procesamiento;

d) Velen por que se incorporen el respeto del derecho a la privacidad y otros derechos humanos reconocidos internacionalmente en el diseño, funcionamiento, evaluación y regulación de las tecnologías de adopción automatizada de decisiones y aprendizaje automático y prevean recursos para compensar por los abusos de los derechos humanos que puedan causar o a los que puedan contribuir;

e) Velen por que las personas tengan acceso a sus datos personales, y adopten las medidas adecuadas para que sea posible modificarlos, corregirlos, actualizarlos, suprimirlos y retirar el consentimiento en relación con ellos, en particular si esos datos son incorrectos o inexactos, o si se obtuvieron ilegalmente;

f) Establezcan salvaguardias adecuadas para prevenir o mitigar los efectos perjudiciales en los derechos humanos que estén directamente relacionados con sus operaciones, productos o servicios, incluso, cuando sea necesario, por medio de cláusulas contractuales o de la notificación a las entidades pertinentes de cualesquiera abusos o violaciones cuando se detecte que sus productos o servicios se han utilizado indebidamente;

g) Aumenten las iniciativas para combatir la discriminación ocasionada por el uso de sistemas de inteligencia artificial, incluso ejerciendo la debida diligencia en la evaluación, prevención y mitigación de los efectos adversos de su despliegue para los derechos humanos;

10. *Alienta* a las empresas a que procuren habilitar soluciones técnicas que aseguren y protejan la confidencialidad de las comunicaciones digitales, como medidas de cifrado, uso de pseudónimos y anonimato, y exhorta a los Estados a que no interfieran en la utilización de esas soluciones técnicas, cerciorándose de que cualesquiera restricciones que hayan de imponerles cumplan con las obligaciones que incumben a los Estados con arreglo al derecho internacional de los derechos humanos, y a que aprueben políticas que reconozcan y protejan la privacidad de las comunicaciones digitales de las personas;

11. *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;

12. *Alienta* a los Estados Miembros y a todos los interesados pertinentes a que prevengan el daño a las personas causado por los sistemas de inteligencia artificial y se abstengan o dejen de usar aplicaciones de inteligencia artificial que son imposibles de operar en consonancia con el derecho internacional de los derechos humanos o que suponen riesgos indebidos para el disfrute de los derechos humanos, en particular el derecho a la privacidad, a menos y hasta que existan las salvaguardias adecuadas para proteger los derechos humanos y las libertades fundamentales;

13. *Alienta* a los Estados, las empresas y otros agentes privados a que impulsen, apoyen y faciliten la educación y la alfabetización digital, promuevan la concienciación sobre los riesgos y la formación y orientación en materia de autoprotección, y apoyen las iniciativas de fomento de la capacidad para que los ciudadanos comprendan mejor los conceptos relacionados con la inteligencia artificial, la transparencia y la explicabilidad, de manera que se garantice el respeto de sus derechos, incluido el derecho a la privacidad;

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 promuevan la participación de las mujeres para hacer frente a la violencia y la discriminación contra las mujeres y las niñas en los contextos digitales, 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 denuncia transparentes y accesibles;

15. *Pone de relieve* que, en la era digital, el cifrado y el anonimato se han hecho esenciales para que muchos periodistas y trabajadores de los medios de comunicación puedan ejercer libremente su labor y disfrutar de sus derechos humanos, en particular sus derechos a la libertad de expresión y a la privacidad, entre ellos el derecho a mantener comunicaciones seguras y a proteger el carácter confidencial de sus fuentes, y exhorta a los Estados a no interferir en el uso que hacen de esas tecnologías los periodistas y trabajadores de los medios de comunicación y a garantizar que cualquier restricción al respecto cumpla con las obligaciones que les incumben en virtud del derecho internacional de los derechos humanos;

16. *Alienta* a todas las partes interesadas pertinentes a que participen en diálogos oficiosos sobre el derecho a la privacidad y toma nota con aprecio de la contribución de la Relatora Especial sobre el derecho a la privacidad a este proceso;

17. *Decide* seguir examinando la cuestión en su octogésimo primer período de sesiones.

*53ª sesión plenaria*
*17 de diciembre de 2024*