



Asamblea General

Distr. limitada
24 de septiembre de 2019
Español
Original: inglés

Consejo de Derechos Humanos

42º período de sesiones

9 a 27 de septiembre de 2019

Tema 3 de la agenda

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

Albania*, Alemania*, Armenia*, Austria, Bélgica*, Brasil, Bulgaria, Chipre*, Colombia*, Croacia, Dinamarca, Eslovaquia, Eslovenia*, España, Estonia*, Finlandia*, Grecia*, Hungría, Irlanda*, Islandia, Letonia*, Liechtenstein*, Lituania*, Luxemburgo*, Malawi*, Malta*, México, Montenegro*, Noruega*, Países Bajos*, Portugal*, Rumania*, San Marino*, Suecia*, Suiza*, Túnez y Ucrania: proyecto de resolución

42/... 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, la Convención sobre los Derechos del Niño, la Convención sobre los Derechos de las Personas con Discapacidad y otros instrumentos internacionales pertinentes en materia de derechos humanos,

Reafirmando también la Declaración y el Programa de Acción de Viena,

Reiterando la universalidad, indivisibilidad, interdependencia e interrelación de todos los derechos humanos y las libertades fundamentales,

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,

Recordando también que las empresas 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,

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 sus informes sobre la cuestión y recordando el seminario

* Estado no miembro del Consejo de Derechos Humanos.



de expertos sobre el derecho a la privacidad en la era digital organizado por la Oficina los días 19 y 20 de febrero de 2018,

Acogiendo con beneplácito también la labor del Relator Especial sobre el derecho a la privacidad y tomando nota de sus informes, así como de las contribuciones a la promoción y protección del derecho a la privacidad realizadas por otros procedimientos especiales del Consejo de Derechos Humanos,

Tomando nota de la estrategia del Secretario General en materia de nuevas tecnologías, incluidos la labor del Panel de Alto Nivel sobre la Cooperación Digital y su informe titulado “La era de la interdependencia digital”, presentado al Secretario General el 10 de junio de 2019,

Tomando nota de la aprobación por el Comité de Alto Nivel sobre Gestión, el 11 de octubre de 2018, de los Principios de Protección de Privacidad y los Datos Personales,

Tomando nota con aprecio de la observación general núm. 16 (1988) del Comité de Derechos Humanos sobre el derecho a la intimidad y su recomendación de 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, y observando al mismo tiempo los grandes avances tecnológicos que se han producido desde su aprobación y la necesidad de ocuparse del derecho a la privacidad a la vista de los problemas que presenta la era digital,

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 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 y 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, y observando con preocupación que las violaciones o transgresiones del derecho a la privacidad podrían afectar al ejercicio de 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 asociación pacíficas,

Recordando que la Asamblea General, en su resolución 73/179, de 17 de diciembre de 2018, alentó al Consejo de Derechos Humanos a que siguiera ocupándose activamente del debate, e invitó a todas las partes interesadas pertinentes a que siguieran examinando la forma en que la elaboración de perfiles, la adopción automatizada de decisiones y las tecnologías de aprendizaje automático, a veces denominadas inteligencia artificial, cuando no contaban con las salvaguardas debidas repercutían en el disfrute del derecho a la privacidad, con el fin de aclarar los principios y las normas existentes y determinar las mejores prácticas de promoción y protección de ese derecho;

Reconociendo que el examen del derecho a la privacidad debe basarse en las obligaciones jurídicas internacionales y nacionales existentes, 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 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 derecho a la privacidad y otros derechos humanos, así como la necesidad de examinar los principios de no arbitrariedad, legitimidad, legalidad, necesidad y proporcionalidad en relación con las prácticas de vigilancia,

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 todos los individuos y tener repercusiones particulares en las mujeres, así como los niños, las personas con discapacidad y las personas vulnerables y marginadas,

Reconociendo la necesidad de que los Gobiernos, el sector privado, las organizaciones internacionales, la sociedad civil, las comunidades técnica y académica y todos los interesados pertinentes conozcan los impactos, las oportunidades y los retos que entraña el cambio tecnológico rápido en la promoción y la protección de los derechos humanos, así como su potencial a los efectos de facilitar la realización de actividades, acelerar el progreso humano y promover y proteger los derechos humanos y las libertades fundamentales,

Observando que la utilización de la inteligencia artificial puede contribuir a la promoción y protección de los derechos humanos y que también puede tener consecuencias a gran escala y de alcance mundial, en particular en lo que respecta al derecho a la privacidad, lo cual está transformando los Gobiernos y las sociedades, los sectores económicos y el mundo del trabajo,

Reconociendo que, a pesar de sus efectos positivos, la utilización de la inteligencia artificial, que requiere el procesamiento de grandes cantidades de datos, a menudo relacionados con datos personales, en particular sobre 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, el rastreo, el establecimiento de perfiles, el reconocimiento facial, la predicción de la conducta y o la calificación de las personas,

Haciendo notar que la utilización de la inteligencia artificial sin las debidas salvaguardias puede entrañar el riesgo de reforzar la discriminación, incluidas las desigualdades estructurales,

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

Observando con preocupación que el procesamiento automático de datos personales para la elaboración de perfiles, la adopción automatizada de decisiones y las tecnologías de aprendizaje automático puede dar lugar, si no median las debidas salvaguardias, a discriminaciones o a decisiones que por lo demás pueden afectar al goce de los derechos humanos, incluidos los derechos económicos, sociales y culturales, y reconociendo la necesidad de que se aplique el derecho internacional de los derechos humanos cuando se conciben, se desarrollen, se desplieguen, se evalúen y se regulen esas tecnologías y se vele por que se sometan a las salvaguardas y la supervisión apropiadas,

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

Poniendo de relieve que la vigilancia y/o la interceptación ilegales o arbitrarias de las comunicaciones, la recopilación ilegal o arbitraria de datos personales o el pirateo ilegal o arbitrario 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,

Poniendo de relieve también 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 y cuando compartan los datos reunidos, entre otras cosas, mediante acuerdos de intercambio de información confidencial 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 recopilación de información biométrica delicada 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 aplicando políticas de protección de datos y salvaguardias,

Observando también que, si bien la prevención y represión del terrorismo y del extremismo violento conducente al terrorismo revisten gran importancia para el interés público, y que la preocupación por la seguridad pública puede justificar la reunión y protección de cierta información delicada, los Estados deben velar por el pleno cumplimiento de las obligaciones que les incumben en virtud del derecho internacional de los derechos humanos,

Poniendo de relieve que, en la era digital, puede ser importante contar con soluciones técnicas para asegurar y proteger la confidencialidad de las comunicaciones digitales, incluidas 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 expresión y la libertad de reunión y de asociación pacíficas, y reconociendo que los Estados deben abstenerse de recurrir a técnicas de vigilancia ilícitas o arbitrarias,

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

3. *Reconoce* la naturaleza global y abierta de Internet y el rápido avance de la tecnología de la información y las comunicaciones como fuerza impulsora de la aceleración de los progresos hacia el desarrollo en sus distintas formas, incluido el logro de los Objetivos de Desarrollo Sostenible;

4. *Afirma* que los derechos de las personas también deben estar protegidos en Internet, incluido el derecho a la privacidad;

5. *Reconoce* que la utilización, el despliegue y el ulterior desarrollo de tecnologías nuevas y emergentes, como la inteligencia artificial, pueden afectar al disfrute del derecho a la privacidad y de otros derechos humanos, y que los riesgos para el derecho a la privacidad pueden y deben reducirse al mínimo mediante la adopción de una normativa adecuada o de otros mecanismos apropiados, entre otras cosas, teniendo en cuenta el derecho internacional de los derechos humanos cuando se conciben, se desarrollen y se desplieguen tecnologías nuevas y emergentes, tales como la inteligencia artificial, garantizando la existencia de una infraestructura de datos sin riesgos, segura y de gran calidad y estableciendo mecanismos de verificación de datos centrados en la actividad de la actividad del ser humano y mecanismos de resarcimiento;

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;

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, en particular 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, con miras a 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 sean compatibles con los principios de legalidad, necesidad y proporcionalidad, y cumplan las obligaciones que les incumben en virtud del derecho internacional;

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) 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 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, incluidas, con repercusiones particulares, las mujeres, así como los niños y las personas en situaciones vulnerables o los grupos marginados;

i) 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;

j) 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 de 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;

k) Consideren 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;

l) 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;

m) 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;

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 recopilen, almacenen, utilicen, compartan y procesen datos a que:

a) Cumplan su responsabilidad 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;

b) Informen a los usuarios sobre la recopilación, la utilización, la distribución y la retención de sus datos que puedan afectar a su derecho a la privacidad y establezcan un régimen de transparencia y políticas que permitan el consentimiento informado de los usuarios, según proceda;

c) Apliquen salvaguardas 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 indemnizaciones por las transgresiones de los derechos humanos que hayan causado o a las que hayan contribuido;

f) Establezcan salvaguardias adecuadas para prevenir o mitigar los efectos negativos en los derechos humanos que estén directamente relacionados con sus operaciones, productos o servicios, en particular, 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;

9. *Alienta* a las empresas a que traten de encontrar soluciones técnicas propicias para asegurar y proteger la confidencialidad de las comunicaciones digitales, que puedan incluir medidas de codificación y anonimato, y exhorta a los Estados a no interferir en el uso de esas soluciones técnicas, y que cualquier restricción a las mismas se ajuste a las obligaciones que tienen los Estados en virtud del derecho internacional de los derechos humanos;

10. *Solicita* a la Alta Comisionada de las Naciones Unidas para los Derechos Humanos que organice, antes del 44º período de sesiones del Consejo de Derechos Humanos, un seminario de expertos de un día de duración para examinar la forma en que la inteligencia artificial y, en particular, la elaboración de perfiles, la adopción automatizada de decisiones y las tecnologías de aprendizaje automático, pueden, sin las debidas salvaguardias, repercutir en el goce del derecho a la privacidad, prepare un informe temático sobre el tema y lo presente al Consejo de Derechos Humanos en su 45º período de sesiones;

11. *Alienta* a los Estados, los organismos, fondos y programas competentes de las Naciones Unidas, las organizaciones intergubernamentales, los órganos creados en virtud de tratados, los procedimientos especiales, los mecanismos regionales de derechos humanos, las organizaciones de la sociedad civil, el mundo académico, las instituciones nacionales de derechos humanos, las empresas, la comunidad técnica y otros interlocutores pertinentes a participar activamente en el taller de expertos;

12. *Decide* seguir examinando la cuestión en relación con el mismo tema de la agenda.
