Naciones Unidas A/HRC/28/39

Asamblea General

Distr. general
19 de diciembre de 2014
Español
Original: inglés

Consejo de Derechos Humanos
28º período de sesiones
Temas 2 y 3 de la agenda
Informe anual del Alto Comisionado de las Naciones Unidas para los Derechos Humanos e informes de la Oficina del Alto Comisionado y del Secretario General

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

Resumen de la mesa redonda del Consejo de Derechos Humanos sobre el derecho a la privacidad en la era digital

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

Resumen

Este informe se presenta en cumplimiento de la decisión 25/117 del Consejo de Derechos Humanos. Contiene un resumen de la mesa redonda sobre el derecho a la privacidad en la era digital, celebrada el 12 de septiembre de 2014 durante el 27º período de sesiones del Consejo de Derechos Humanos. Atendiendo a la petición formulada por el Consejo de Derechos Humanos, durante la mesa redonda se examinó la cuestión de la promoción y protección del derecho a la privacidad en la era digital en el contexto de la vigilancia nacional y extraterritorial, la interceptación de comunicaciones digitales y la recopilación de datos personales, en particular a gran escala, entre otras cosas para detectar dificultades y mejores prácticas, tomando en consideración el informe de la Alta Comisionada de las Naciones Unidas para los Derechos Humanos

GE.14-24711 (S) 150115 160115
1424711

Índice

I. Introducción

1. En cumplimiento de su decisión 25/117, el Consejo de Derechos Humanos celebró una mesa redonda sobre el derecho a la privacidad en la era digital el 12 de septiembre de 2014. En el debate se tuvieron en cuenta las cuestiones planteadas en el informe presentado por la Alta Comisionada de las Naciones Unidas para los Derechos Humanos al Consejo de Derechos Humanos en su 27º período de sesiones (A/HRC/27/37).

2. Atendiendo a la petición formulada por el Consejo de Derechos Humanos, durante la mesa redonda se examinó la cuestión de la promoción y la protección del derecho a la privacidad en la era digital en el contexto de la vigilancia nacional y extraterritorial, la interceptación de comunicaciones digitales y la recopilación de datos personales, en particular a gran escala, entre otras cosas para detectar dificultades y mejores prácticas, tomando en consideración el informe de la Alta Comisionada para los Derechos Humanos.

3. La mesa redonda estuvo presidida por el Presidente del Consejo de Derechos Humanos y moderada por Marko Milanovic, profesor asociado de la Universidad de Nottingham. La Alta Comisionada Adjunta de las Naciones Unidas para los Derechos Humanos pronunció el discurso de apertura. Los participantes en la mesa redonda fueron la Sra. Catalina Botero, Relatora Especial sobre la libertad de expresión de la Comisión Interamericana de Derechos Humanos; la Sra. Sarah Cleveland, titular de la Cátedra Louis Henkin de Derechos Humanos y Constitucionales de la Facultad de Derecho de la Universidad de Columbia; el Sr. Yves Nissim, Director Adjunto de Responsabilidad Social Empresarial de Orange y ex Presidente del Diálogo de la Industria de las Telecomunicaciones, y la Sra. Carly Nyst, Directora Jurídica de Privacy International.

4. En su decisión 25/117, el Consejo solicitó a la Oficina del Alto Comisionado que le presentara un informe resumido de la mesa redonda en su 28º período de sesiones. Este informe se presenta en respuesta a esa petición.

II. Discurso de apertura de la Alta Comisionada Adjunta de las Naciones Unidas para los Derechos Humanos

5. La Alta Comisionada Adjunta indicó que, en muy poco tiempo, las tecnologías de las comunicaciones digitales habían revolucionado la manera en que los seres humanos interactuaban y que, para millones de personas, la era digital constituía la era de la emancipación, quizás el mayor movimiento de liberación que el mundo hubiera conocido. Señaló, a modo de ejemplo, que más de un millón de personas había participado de manera electrónica en el diálogo abierto y en las consultas que se estaban llevando a cabo con el fin de elaborar un marco para los objetivos de desarrollo sostenible para después de 2015, en que se pedía la plena inclusión de los derechos humanos. Destacó que los defensores de los derechos humanos, los activistas, las voces democráticas y las minorías, entre otros, ahora podían comunicarse a través de plataformas digitales y participar en el debate mundial de maneras que antes resultaban inconcebibles.

6. La Alta Comisionada Adjunta también señaló que dichas plataformas digitales eran vulnerables a la vigilancia, la interceptación y la recopilación de datos. Se había expresado gran preocupación por el hecho de que en todo el mundo hubieran salido a la luz políticas y prácticas que explotaban esa vulnerabilidad. Añadió que las prácticas de vigilancia podían tener efectos muy reales sobre los derechos humanos de las personas, en particular sus derechos a la intimidad, a la libertad de expresión y de opinión, a la libertad de reunión, a la vida familiar y a la salud. En particular, la información recopilada mediante la vigilancia digital había sido utilizada para atacar a disidentes, y había información fidedigna según la

cual las tecnologías digitales habían sido empleadas para recabar información que había conducido a la comisión de actos de tortura y otras formas de malos tratos.

7. La Alta Comisionada Adjunta recordó que, en su resolución 68/167, la Asamblea General había solicitado a la Alta Comisionada que presentara un informe sobre "la protección y la promoción del derecho a la privacidad en el contexto de la vigilancia y la interceptación de las comunicaciones digitales y la recopilación de datos personales en los planos nacional y extraterritorial, incluso a gran escala", informe que fue presentado al Consejo de Derechos Humanos en su 27º período de sesiones. El informe se basó en consultas de expertos y en investigaciones exhaustivas sobre la legislación y la jurisprudencia existentes a nivel nacional e internacional, así como en información procedente de una gran variedad de fuentes, incluidas las respuestas a un cuestionario enviado a las partes interesadas.

8. Como se indicó claramente en el informe, el derecho internacional de los derechos humanos constituía un marco sólido y universal para la promoción y la protección del derecho a la privacidad, también en el contexto de la vigilancia nacional y extraterritorial, la interceptación de las comunicaciones digitales y la recopilación de datos personales. Sin embargo, las prácticas observadas en muchos Estados ponían de manifiesto la ausencia de leyes nacionales adecuadas y de medidas para garantizar su aplicación, así como la insuficiencia de garantías de procedimiento y la ineficacia de los sistemas de supervisión, lo que contribuía a generalizar la impunidad por las injerencias arbitrarias o ilegales en el derecho a la privacidad.

9. La Alta Comisionada Adjunta recordó que el informe de la Alta Comisionada examinaba la protección que ofrecía el derecho internacional de los derechos humanos en materia de privacidad, y particularmente qué significaba la expresión "injerencia en la privacidad" en el contexto de las comunicaciones en línea, qué constituía una injerencia "arbitraria e ilegal" en ese contexto y a quién asistían esos derechos, y dónde. Por ejemplo, con respecto a qué es lo que constituía una injerencia en la privacidad, era evidente que la agregación de los datos de las comunicaciones podría dar información exhaustiva sobre el comportamiento de una persona, sus relaciones sociales, sus preferencias personales y su identidad, más incluso que la información obtenida al leer el correo electrónico de una persona. La reunión y conservación de datos de las comunicaciones podría, por lo tanto, constituir una injerencia en la privacidad, independientemente de si dichos datos fueran o no consultados o utilizados. La mera existencia de un programa de vigilancia en masa en relación con las comunicaciones por correo electrónico y otras formas de expresión digital suponía una injerencia en la privacidad, e incumbía al Estado demostrar que tal injerencia no era ni ilegal ni arbitraria.

10. En cuanto a las injerencias "arbitrarias" o "ilegales" en la privacidad, en el informe se señalaba que la vigilancia de los datos de las comunicaciones electrónicas llevada a cabo por el Estado podría constituir una medida legítima de control, si se realizaba en cumplimiento de la ley. No obstante, los Estados debían demostrar que la vigilancia era necesaria y proporcional al riesgo concreto de que se tratara. La conservación obligatoria de datos por terceros, en virtud de la cual se exigía a las empresas de telefonía y a los proveedores de servicios de Internet que almacenaran metadatos sobre las comunicaciones de sus clientes, para que las fuerzas del orden y los organismos de inteligencia pudieran acceder posteriormente a ellos, no parecía necesaria ni proporcionada.

11. Como se subrayaba en el informe, la Alta Comisionada Adjunta recordó que los Estados tenían la obligación de asegurar que la privacidad de las personas estuviera protegida por ley contra las injerencias ilegales o arbitrarias. Todas las formas de vigilancia de las comunicaciones debían ajustarse a una ley que fuera públicamente accesible y, a su vez, esa ley debía ser conforme al régimen constitucional del Estado en cuestión y al derecho internacional de los derechos humanos. Las normas e interpretaciones secretas de

la ley, incluso las realizadas por jueces, no eran compatibles con el principio según el cual las leyes debían ser claras y accesibles. Tampoco lo eran las leyes o normas que concedieran una facultad discrecional excesiva a las autoridades ejecutivas, como los servicios de seguridad e inteligencia.

12. La Alta Comisionada Adjunta también mencionó las preocupaciones planteadas en el informe respecto de la vigilancia extraterritorial y la interceptación de comunicaciones digitales. Sobre la base de la labor del Comité de Derechos Humanos y la Corte Internacional de Justicia respecto de la determinación del momento en que un Estado ejerce su jurisdicción, en el informe se señaló que las obligaciones de derechos humanos de un Estado se materializaban cada vez que este ejercía su poder o control efectivo. Si la vigilancia entrañaba el ejercicio del poder o el control efectivo de un Estado en relación con una infraestructura de comunicaciones digitales, entonces esa vigilancia, dondequiera que se produjera, materializaría las obligaciones del Estado en materia de derechos humanos. Ello incluiría, por ejemplo, las escuchas directas o la infiltración de una infraestructura de comunicaciones y el ejercicio por el Estado de su jurisdicción reguladora sobre un tercero que tuviera el control material de los datos.

13. En el informe se recordaba que el derecho internacional de los derechos humanos también era explícito en relación con el principio de no discriminación, y que los Estados debían tomar medidas para garantizar que toda injerencia en el derecho a la privacidad se ajustara a los principios de legalidad, proporcionalidad y necesidad, con independencia del origen étnico, la nacionalidad, el emplazamiento o cualquier otra característica de las personas cuyas comunicaciones estuvieran siendo supervisadas.

14. En el informe también se indicaba que las garantías de procedimiento y una supervisión eficaz eran fundamentales para proteger el derecho a la privacidad en la legislación y en la práctica. La inexistencia de una supervisión eficaz había fomentado la impunidad por las injerencias arbitrarias o ilegales en el derecho a la privacidad en el entorno digital. Las garantías internas que no iban acompañadas de una supervisión independiente habían demostrado su ineficacia frente a los métodos de vigilancia ilegales o arbitrarios. Para que fueran adecuadas, las garantías debían incluir una supervisión civil independiente y la participación de todos los poderes del Estado, a fin de asegurar la protección efectiva de la ley. Los Estados también tenían la obligación jurídica de proporcionar recursos efectivos, ya fueran judiciales, legislativos o administrativos, con procedimientos conocidos y accesibles, en caso de violación de la privacidad mediante actividades de vigilancia digital.

15. Por último, la Alta Comisionada Adjunta se refirió a la función del sector privado, una cuestión que también se abordaba en el informe de la Alta Comisionada. Los gobiernos recurrían cada vez más a empresas privadas para llevar a cabo y facilitar la vigilancia digital. En algunos casos podía haber razones legítimas para que una empresa proporcionara los datos de sus usuarios. Sin embargo, cuando la solicitud contravenía el derecho de los derechos humanos, o si la información se utilizaba en violación de ese derecho, la empresa en cuestión corría el riesgo de ser cómplice de abusos contra los derechos humanos. Los Principios Rectores sobre las Empresas y los Derechos Humanos, aprobados por el Consejo de Derechos Humanos en su resolución 17/4, de 16 de junio de 2011, proporcionaban un marco internacional para prevenir y combatir los efectos adversos de las actividades empresariales en los derechos humanos. Dejaban claro que la responsabilidad de proteger los derechos humanos se aplicaba a todas las operaciones que la empresa realizara en todo el mundo, independientemente de la ubicación de sus usuarios y de si el Estado en cuestión cumplía sus propias obligaciones de derechos humanos. Al parecer, muchas empresas no eran suficientemente conscientes de esas cuestiones.

16. La Alta Comisionada Adjunta concluyó señalando que la falta de transparencia de los gobiernos en relación con las medidas adoptadas por ellos que pudieran afectar al derecho a la privacidad solía dificultar considerablemente los intentos por subsanar las carencias y hacer efectiva la rendición de cuentas. Llegó a la conclusión de que existía una necesidad evidente de proseguir los debates y ahondar en los análisis a medida que la información relativa a esas medidas se fuera haciendo pública.

III. Contribuciones de los participantes en la mesa redonda

17. En respuesta a las preguntas formuladas por el moderador, las observaciones iniciales de los participantes se centraron en cuestiones vinculadas al marco del derecho internacional de los derechos humanos en relación con el derecho a la privacidad, incluidas las garantías de procedimiento, la supervisión eficaz y el derecho a un recurso, así como la función del sector empresarial.

18. La Directora Jurídica de Privacy International puso de relieve la importancia de la privacidad en toda sociedad democrática y destacó los vínculos existentes entre la privacidad y el concepto de dignidad humana. Señaló que el derecho a la privacidad era un requisito fundamental para el disfrute de otros derechos, así como garante de los mismos, ya que permitía a las personas desarrollar de manera independiente pensamientos e ideas y expresarlos libremente, elegir qué religión profesar y a qué partido político dar su apoyo. La Sra. Nyst explicó que el derecho a la privacidad se había expresado por primera vez en el derecho internacional en la Declaración Universal de Derechos Humanos, donde los redactores tuvieron clara no solo la necesidad de incluir el derecho a la privacidad, sino también la importancia del derecho a la privacidad de las comunicaciones, como se desprende de los trabajos preparatorios de la Declaración.

19. La Sra. Nyst señaló que muchas de las acciones corrientes que se realizaban a diario incluían una "comunicación", como el envío de un correo electrónico o un mensaje de texto, el acceso a una cuenta bancaria, la búsqueda de información en Internet o el acceso a los servicios públicos. Cualquier comunicación digital implicaba el viaje de datos privados por todo el mundo, y a través de los cables de muchas empresas privadas, antes de llegar a su destino. El reto que la tecnología planteaba a la privacidad era asegurar que la obligación del Estado de respetar, hacer efectivo y proteger el derecho a la privacidad y las responsabilidades del sector privado fueran significativas en la era digital. La oradora señaló que el marco jurídico ya existía, puesto que el derecho a la privacidad estaba consagrado en la mayoría de los tratados internacionales y regionales de derechos humanos y en muchas constituciones nacionales, y que se necesitaba un nuevo entendimiento de la manera en que se aplicaban esos textos.

20. La Relatora Especial sobre la libertad de expresión de la Comisión Interamericana de Derechos Humanos se refirió a las posibilidades que había creado Internet para la libertad de expresión, la comunicación y el intercambio de información. Señaló que, al mismo tiempo, también se había facilitado el registro, el almacenamiento y la administración de enormes cantidades de datos. Esa información, ya fueran datos de contenido o metadatos, podría ser muy reveladora hasta de los aspectos más íntimos de la vida privada de las personas o las comunidades. La oradora indicó que los marcos jurídicos no habían seguido el ritmo de los adelantos tecnológicos en la era digital, y subrayó la necesidad de regular tanto la recopilación como el análisis de la información, teniendo en cuenta la libertad de expresión, el derecho a la privacidad y otros derechos humanos pertinentes.

21. La Sra. Botero observó además que las políticas de vigilancia podían tener repercusiones sobre una gama más amplia de derechos humanos. Se refirió a los efectos de la vigilancia sobre el derecho a la libertad de expresión, bien directamente, cuando el derecho no pudiera ejercerse de forma anónima como consecuencia de la vigilancia, o indirectamente, porque la mera existencia de la vigilancia podría tener un efecto disuasivo, infundir miedo e inhibición y hacer que las personas tuvieran cuidado con lo que decían y hacían. La oradora explicó que, dado que el derecho a la libertad de expresión constituía una plataforma de cara a otros derechos, su vulneración podría dar lugar a la violación de otros derechos, como la libertad de asociación, la libertad de reunión, la libertad religiosa y el derecho a la salud. Debido a las posibles repercusiones de las actividades de vigilancia en toda la estructura de los derechos humanos, era necesario que los Estados revisaran su legislación para establecer límites a los programas de vigilancia, que deberían incluir el respeto de los principios de necesidad y proporcionalidad, así como mecanismos de supervisión adecuados. La Sra. Botero explicó que, como Internet era un medio de comunicación especial y único que permitía el ejercicio libre, plural y democrático del derecho a la libertad de expresión, su gobernanza era una cuestión especialmente importante. La oradora señaló que, para asegurar que todos los puntos de vista pertinentes pudieran ser tenidos debidamente en cuenta, los Estados debían garantizar la participación equitativa de todos los agentes competentes que participaban en la gobernanza de Internet y fomentar el fortalecimiento de la cooperación entre las autoridades, el mundo académico, la sociedad civil, las comunidades científica y técnica y el sector privado, tanto a nivel nacional como internacional.

22. La titular de la Cátedra Louis Henkin de Derechos Humanos y Constitucionales de la Facultad de Derecho de la Universidad de Columbia indicó que todas las personas, independientemente de su ubicación o nacionalidad, estaban protegidas por los derechos humanos, que eran universales e inherentes a la dignidad humana. La oradora señaló que, en ocasiones, las prácticas de vigilancia del Estado distinguían entre ciudadanos y no ciudadanos. A ese respecto, la Sra. Cleveland destacó que, como había reconocido el Comité de Derechos Humanos, el principio de no discriminación que figuraba en el artículo 2 del Pacto Internacional de Derechos Civiles y Políticos protegía a los ciudadanos y los no ciudadanos por igual[1]. Por consiguiente, ni los ciudadanos ni los no ciudadanos podían ser objeto de injerencias ilegales o arbitrarias en su privacidad. La oradora también señaló que, con frecuencia, los Estados ejercían la vigilancia en su propio territorio para reprimir la libertad de expresión y de asociación, o para castigar a periodistas, disidentes y otras personas críticas con el gobierno. De conformidad con el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, los Estados tenían la obligación de respetar y garantizar el derecho a la privacidad de todas las personas que se encontraran en su territorio y estuvieran sujetas a su jurisdicción.

23. La Sra. Cleveland destacó que, tal y como habían reconocido la Corte Internacional de Justicia[2] y el Comité de Derechos Humanos[3], las garantías incluidas en el Pacto Internacional de Derechos Civiles y Políticos se aplicaban a las personas que estuvieran sometidas de algún modo a la jurisdicción de un Estado. Esa era también la interpretación que mejor conciliaba el texto del Pacto Internacional de Derechos Civiles y Políticos con su contenido, objeto y finalidad. El Comité de Derechos Humanos había reconocido hacía

[1] Véase la observación general Nº 18 (1989) del Comité de Derechos Humanos, relativa a la no discriminación.

[2] Véase la opinión consultiva de la Corte Internacional de Justicia sobre las consecuencias jurídicas de la construcción de un muro en el Territorio Palestino Ocupado, informe de 2004, pág. 136, y el fallo dictado en relación con las actividades armadas en el territorio del Congo *(República Democrática del Congo c. Uganda)*, informe de 2005, pág. 168.

[3] Véase la observación general Nº 31 (2004) del Comité de Derechos Humanos, sobre la índole de la obligación jurídica general impuesta a los Estados partes en el Pacto.

mucho tiempo que un Estado no podía eludir sus obligaciones internacionales en materia de derechos humanos mediante la adopción de medidas fuera de su territorio que tendría prohibido tomar dentro de sus fronteras. La Sra. Cleveland explicó que la actividad cibernética traspasaba los límites territoriales, que la vigilancia digital podía incluir el simple ejercicio del control físico de una persona o territorio por el Estado e implicar la adopción de medidas en un lugar que afectaran a una persona en otro lugar. La oradora subrayó que esa conducta podría afectar a las obligaciones de derechos humanos de un Estado. Por último, la oradora señaló que el hecho de que el derecho a la privacidad se aplicara a los no ciudadanos o a los nacionales en el extranjero no significaba que las actividades de vigilancia siempre fueran ilegales de por sí. Toda restricción del derecho a la privacidad para atender los intereses legítimos de un Estado en materia de seguridad o de aplicación de la ley había de adoptarse teniendo plenamente en cuenta los requisitos para hacerlo, de conformidad con lo dispuesto en el derecho internacional de los derechos humanos; en particular, dicha restricción no debía ser arbitraria o ilegal.

24. En relación con el papel del sector privado, el moderador, Sr. Milanovic, señaló que las empresas privadas agregaban datos para sus propios fines y también podrían ser invitadas a participar en proyectos gubernamentales. Centrándose en la relación entre los gobiernos y las empresas de telecomunicaciones privadas, preguntó cómo deberían responder las empresas privadas a las solicitudes de los gobiernos. El Director Adjunto de Responsabilidad Social Empresarial de Orange observó que los problemas derivados de las diversas solicitudes que podría recibir una empresa de telecomunicaciones para reunir o conservar datos sobre sus clientes o para preparar sus redes a fin de facilitar las escuchas se hicieron más patentes durante la Primavera Árabe. Algunas empresas de telecomunicaciones habían recibido solicitudes de gobiernos (en algunos casos, a punta de pistola) que podrían haber afectado a los derechos a la libertad de expresión y a la privacidad de sus clientes. Esa situación había llevado a esas empresas a crear el Diálogo de la Industria de las Telecomunicaciones sobre la Libertad de Expresión y la Privacidad, con el fin de abordar conjuntamente cuestiones relacionadas con la libertad de expresión y el derecho a la privacidad en el sector de las telecomunicaciones[4]. El 12 de marzo de 2013, el Diálogo había publicado diez principios rectores que se inspiraban 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". Los principios publicados por el Diálogo abordaban la privacidad y la libertad de expresión en la medida en que se relacionaban con el sector de las telecomunicaciones, y en particular estudiaban la interacción y los límites que había entre la obligación de un gobierno de proteger los derechos humanos y la responsabilidad de las empresas de telecomunicaciones de respetar los derechos humanos.

25. En lo que respecta a las dificultades, el Sr. Nissim destacó que las empresas de telecomunicaciones tenían mucho personal sobre el terreno en distintos países, y que su seguridad era una prioridad absoluta, como se reconocía en el quinto principio rector[5]. También indicó que, si bien las empresas que participaban en el Diálogo de la Industria de las Comunicaciones deseaban defender los derechos humanos, en particular la libertad de expresión y el derecho a la privacidad, era importante recordar que habían concertado acuerdos de licencia con los gobiernos y estaban sujetas a las leyes y reglamentos nacionales. Debido a la necesidad de proteger a su personal que se encontraba en esos países, las empresas tenían que poder entablar un diálogo con los gobiernos anfitriones cuando fuera necesario. Señaló que había tres cuestiones urgentes que era necesario resolver. En primer lugar, los gobiernos no deberían solicitar ni obtener el acceso directo a

[4] El Diálogo de la Industria de las Telecomunicaciones está integrado actualmente por siete operadores y dos proveedores. Véase www.telecomindustrydialogue.org.

[5] El principio 5 establecía que las empresas de comunicaciones deberían "buscar siempre el garantizar la seguridad y la libertad de los empleados de la compañía que [pudieran] estar expuestos a situaciones de riesgo".

la red de telecomunicaciones. En segundo lugar, el proceso mediante el cual los gobiernos podían formular solicitudes a las empresas de telecomunicaciones debería ser claro y transparente. En tercer lugar, si bien las empresas de telecomunicaciones estaban dispuestas a ser transparentes con respecto a las solicitudes que recibían, la transparencia era, ante todo, responsabilidad de los gobiernos.

26. En cuanto a las condiciones para que la restricción del derecho a la privacidad y la libertad de expresión fuera legítima, la Sra. Botero explicó que toda limitación debía establecerse de antemano por ley. Esas leyes debían definir con precisión las causas y condiciones que permitirían al Estado interceptar las comunicaciones de los particulares, reunir datos sobre las comunicaciones o someterlas a una vigilancia o supervisión que repercutiría en el derecho a la privacidad. La ley no debía ser imprecisa o ambigua, ni conceder amplias facultades discrecionales al poder ejecutivo en su interpretación. También debía proporcionar garantías en relación con la naturaleza, el alcance y la duración de las medidas de vigilancia. Las limitaciones impuestas al derecho a la privacidad también debían tener un objetivo legítimo. En el caso de la vigilancia, los motivos que con mayor probabilidad esgrimirían los Estados eran la seguridad nacional y la lucha contra la delincuencia. Toda limitación debía ser proporcional y estrictamente necesaria. Ello significaba que había que establecer claramente la existencia de una necesidad verdadera y urgente de imponer la limitación, y que no era posible lograr el objetivo en cuestión mediante cualquier otra medida menos restrictiva. En cualquier caso, los derechos solo deberían limitarse cuando el riesgo que corría el interés protegido, en sentido estricto, era mayor que el interés general por mantener el derecho a la intimidad y la libertad de expresión. La Sra. Botero también señaló que los criterios deberían ser aún más estrictos cuando los derechos protegidos estuvieran relacionados con los aspectos más íntimos de la vida privada de las personas. A fin de garantizar la protección de los principios de legalidad, proporcionalidad y necesidad, toda decisión de llevar a cabo actividades de vigilancia que limitaran el derecho a la privacidad y otros derechos debería ser autorizada por una autoridad judicial independiente.

27. Con respecto a la proporcionalidad, la Sra. Cleveland observó que las medidas deberían ser proporcionales a la importancia de los intereses que estuvieran en juego: el interés del Estado en aplicar la medida y el interés de privacidad de la persona. La oradora explicó que, cuanto más acuciante fuera el interés de privacidad de la persona, más estrictamente debería ajustarse la medida. Se refirió a la jurisprudencia del Tribunal Europeo de Derechos Humanos, que confería a los Estados un margen discrecional razonable, especialmente en la esfera de la seguridad nacional, para que determinaran en cada caso qué medidas eran necesarias y proporcionales para la consecución de un interés particular del Estado. La Sra. Cleveland señaló también la importancia de las garantías procesales establecidas por el Estado para asegurar que el régimen de vigilancia se estuviera aplicando debidamente. Indicó que era necesario que hubiera garantías legales que definieran el régimen, así como medidas de supervisión y recursos retroactivos para asegurar que no se abusara de él.

28. El Sr. Milanovic observó que, a menudo, los Estados distinguían entre la recopilación del contenido de una comunicación, por una parte, y los datos sobre la comunicación, o metadatos, por la otra, y que el primero disfrutaba de mayores garantías que los segundos. Preguntó si esas distinciones eran pertinentes en el marco de las comunicaciones digitales. La Sra. Nyst observó que había que dejar de lado esas distinciones de manera inequívoca, puesto que reflejaban una comprensión desfasada de la naturaleza de las comunicaciones actuales y la incapacidad de actualizar la legislación en consecuencia. Señaló que esas distinciones se remontaban a una época en la que efectivamente existía una diferencia entre el envoltorio y su contenido, mientras que, en el contexto de las comunicaciones digitales, ese envoltorio, es decir, los metadatos, contenía información muy delicada, valiosa y amplia. Por ejemplo, esa información podía ser

extraída de los metadatos y analizada para obtener información sobre las creencias políticas o religiosas de una persona. La oradora se refirió a un estudio realizado por la Universidad de Stanford, en el que se mostraba que era posible obtener información médica, financiera y jurídica de los metadatos. Hizo hincapié en que, por consiguiente, urgía la necesidad de reevaluar esa distinción, como se señalaba en el informe de la Alta Comisionada. La Sra. Nyst indicó que se habían realizado progresos en varios países, que habían reconocido la necesidad de aumentar la protección de los metadatos. También señaló que el Tribunal de Justicia de la Unión Europea había declarado inválida la Directiva sobre la conservación de datos[6] y llegado a la conclusión de que había una tendencia hacia el aumento de la protección de los metadatos. No obstante, la Sra. Nyst destacó que se necesitaba una mayor orientación sobre cómo adaptar las leyes nacionales en consecuencia.

29. Desde la perspectiva de los operadores, el Sr. Nissim dijo que, con frecuencia, las empresas de telecomunicaciones conservaban datos como los rastreos de llamadas por razones técnicas, a fin de garantizar la calidad de sus redes y servicios. No obstante, señaló que, cuando los gobiernos pedían a las empresas de telecomunicaciones que conservaran la información recabada durante períodos de tiempo más largos, o les facilitaran el acceso a ellos, la información podría utilizarse de forma indebida. Agregó que todo acceso por los gobiernos debería exigir la elaboración de legislación. El Sr. Nissim también indicó que, cuando se alcanzaba el nivel de los "macrodatos", y si se aseguraba el anonimato de la información, esta podría utilizarse de manera muy positiva, por ejemplo para la planificación urbana y en la esfera de los transportes y las comunicaciones.

IV. Resumen de los debates

30. Durante el debate interactivo, las delegaciones de Alemania (en nombre de Alemania, Austria, el Brasil, Liechtenstein, México, Noruega, los Países Bajos y Suiza), Argelia, Australia, Bélgica, el Canadá, China, Cuba (en nombre del grupo de países de ideas afines), el Ecuador, los Emiratos Árabes Unidos, Eslovenia, los Estados Unidos de América, Estonia, la Federación de Rusia, Francia, la India, Indonesia, Irlanda, Italia, Malasia, el Pakistán (en nombre de la Organización de Cooperación Islámica), el Reino Unido de Gran Bretaña e Irlanda del Norte, Rumania, Sierra Leona, la Unión Europea, Venezuela (República Bolivariana de) y la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) hicieron uso de la palabra. Las declaraciones de Chile, Myanmar y el Uruguay no se pronunciaron debido a la falta de tiempo. Se publicaron copias de sus declaraciones en la extranet del Consejo de Derechos Humanos.

31. Los delegados de las siguientes organizaciones no gubernamentales (ONG) también hicieron uso de la palabra: American Civil Liberties Union (en un comunicado conjunto con Human Rights Watch), Article 19, Asociación para el Progreso de las Comunicaciones y Korea Center for United Nations Human Rights Policy.

A. Observaciones generales sobre el derecho a la privacidad en la era digital

32. Muchas delegaciones destacaron la calidad del informe presentado por la Alta Comisionada sobre el derecho a la privacidad en la era digital y el hecho de que fuera un hito importante en el contexto de los debates en curso. Muchas delegaciones también expresaron su reconocimiento por la labor de la Oficina del Alto Comisionado de las

[6] Véase la sentencia del Tribunal de Justicia de la Unión Europea de 8 de abril de 2014, asuntos acumulados C-293/12 y C-594/12.

Naciones Unidas para los Derechos Humanos (ACNUDH), entre otros, para que el derecho a la privacidad se respetara en la legislación y en la práctica.

33. Muchas delegaciones acogieron con satisfacción la mesa redonda, ya que el tema era oportuno y el debate necesario, teniendo en cuenta que los avances tecnológicos iban por delante de la comprensión de sus consecuencias para los derechos humanos. También se señaló la importancia de los debates celebrados sobre la cuestión por el Consejo de Derechos Humanos, así como en otros foros, como el Foro para la Gobernanza de Internet.

34. Una delegación señaló que había cerca de 3.000 millones de usuarios de Internet en todo el mundo y que la libertad y la seguridad de Internet se habían convertido en una prioridad para todos. Según lo previsto en los objetivos de desarrollo sostenible para después de 2015 y el Programa de Acción en favor de los países menos adelantados para el decenio 2011-2020 (A/CONF.219/3/Rev.1), todos deben tener acceso a Internet de aquí a 2020.

35. En la mayoría de las intervenciones se indicó, como ya se había puesto de manifiesto en el informe de la Alta Comisionada de las Naciones Unidas, que las innovaciones en la tecnología habían tenido un efecto positivo en la libertad de expresión, habían facilitado el debate a nivel mundial y habían fomentado la participación democrática. Se observó que las comunicaciones digitales podían ser instrumentos para facilitar el disfrute de los derechos humanos, habían contribuido al progreso de la civilización humana, y habían creado nuevas oportunidades para la comunicación, el conocimiento y los negocios. La privacidad formaba parte de una sociedad libre, justa y abierta en la que se pudieran expresar libremente las opiniones sin ningún temor de represión o detención.

36. La mayoría de las delegaciones señalaron, sin embargo, que las mismas plataformas tecnológicas también habían mejorado la capacidad de los actores estatales y no estatales para realizar actividades de vigilancia, interceptación y recopilación masiva de datos. Algunas delegaciones señalaron que esas plataformas no solo eran vulnerables a la vigilancia de masas, sino que de hecho la facilitaban. Una ONG señaló que cuando se amenazaba la privacidad en línea, la confianza en Internet desaparecía, privando a todos, incluidos los periodistas, los blogueros y los defensores de los derechos humanos, de la libertad para comunicarse de forma segura, anónima y confidencial, con un efecto inhibitorio en la libertad de expresión. Otra ONG recalcó que para todos, especialmente los que vivían bajo regímenes represivos, la integridad de las comunicaciones era fundamental para la preservación de la libertad individual y la seguridad de la persona, así como los derechos políticos.

37. Se señaló el crecimiento exponencial del poder del Estado en algunos países debido a su infraestructura de tecnología de la información. Algunas delegaciones se centraron en el hecho de que gran parte de las comunicaciones electrónicas en el mundo pasaba por un número limitado de países. A su vez, ello ofrecía la oportunidad de interceptar las comunicaciones privadas. Algunos países habían desarrollado tecnologías que permitían el acceso a gran parte del tráfico de Internet, los registros de llamadas, las agendas electrónicas personales y otros contenidos de las comunicaciones digitales a nivel mundial. También se hizo referencia a las denuncias de que determinados gobiernos intervenían las comunicaciones en grandes acontecimientos. Varios oradores recordaron que la soberanía de los Estados se debía respetar siempre en lo referente a la vigilancia, la interceptación y la recopilación de datos personales.

38. Otras delegaciones observaron que había una tendencia cada vez mayor por parte de algunos gobiernos a utilizar cibertecnologías para controlar a sus propios ciudadanos, en violación de su derecho a la libertad de expresión y el derecho de acceso a la información. Se señaló que los activistas políticos y los miembros de minorías religiosas eran atacados,

detenidos y a veces asesinados. Una ONG señaló que los efectos de la vigilancia en línea se solían sentir fuera de Internet y formaban parte de una tendencia global para restringir el espacio cívico. Actores estatales y privados vigilaban los movimientos de protesta legítimos para socavar actividades pacíficas y los derechos conexos, en particular los derechos a la libertad de expresión y de reunión.

39. La mayoría de las delegaciones reafirmaron que los derechos de las personas fuera de Internet se debían proteger en línea, tal como se establecía en la resolución 68/167 de la Asamblea General y las resoluciones 20/8 y 26/13 del Consejo de Derechos Humanos.

40. La mayoría de las delegaciones consideraban que el derecho a la privacidad era un requisito para poder expresarse libremente y uno de los derechos básicos de una sociedad democrática. Muchas delegaciones señalaron que la vigilancia tenía repercusiones en derechos distintos del derecho a la privacidad, en particular la libertad de expresión y de opinión y la libertad de reunión y de asociación. Se señaló además que la intimidad y la libertad de expresión "se relacionan entre sí y son mutuamente dependientes" (véase el documento A/HRC/23/40, párr. 79) y permitían y facilitaban el desarrollo de otros derechos fundamentales y el desarrollo sostenible. Dos ONG pusieron como ejemplo el daño concreto que la vigilancia electrónica a gran escala podía tener en la labor de los periodistas y los abogados, socavando la libertad de expresión y de asociación y el derecho a un abogado[7]. Una delegación se refirió a los intentos de silenciar a los medios de comunicación. Otra ONG se refirió a los blogueros que afrontaban acusaciones de terrorismo, en parte por cifrar sus comunicaciones y participar en cursos de seguridad digital para asegurar su privacidad.

41. Una delegación señaló que los particulares a menudo no eran conscientes de la medida en que los datos se podían utilizar o compartir, incluso cuando se recopilaban sin su consentimiento. Algunas delegaciones se refirieron al derecho a la protección de datos y al Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal del Consejo de Europa y su Protocolo Adicional como primer instrumento internacional vinculante en materia de protección de datos e importante contribución al derecho a la privacidad. Una delegación se refirió al llamado "derecho al olvido", en el que el deseo legítimo de no estar asociado con un solo aspecto de la vida o el pasado podría entrar en conflicto con el derecho a la información y podría dar lugar a una distorsión de la memoria colectiva.

42. Muchas delegaciones destacaron las medidas adoptadas a nivel nacional para proteger el derecho a la privacidad en la era digital. La UNESCO se refirió a su labor en relación con la privacidad y la libertad de expresión en la era digital, a una publicación sobre la privacidad en Internet y la libertad de expresión y a un estudio amplio sobre cuestiones de Internet, que incluía un enfoque de la libertad de expresión, la privacidad, el acceso al conocimiento y la información y la ética de la sociedad de la información.

B. Protección legal del derecho a la privacidad

43. La mayoría de las delegaciones hicieron hincapié en que el derecho internacional proporcionaba un marco claro para el derecho a la privacidad, consagrado en el artículo 12 de la Declaración Universal de Derechos Humanos y el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos. Muchos observaron, sin embargo, que el ejercicio del derecho a la privacidad era escaso y que se necesitaban medidas concretas para salvaguardar ese derecho. Algunas señalaron que era necesario abordar exhaustivamente el

[7] Human Rights Watch y American Civil Liberties Union, "With liberty to monitor all: how large-scale US surveillance is harming journalism, law and American democracy" (julio de 2014).

acceso unilateral y no autorizado a los datos privados y la vigilancia generalizada y se hicieron llamamientos en favor de que se adoptaran medidas urgentes para detener las prácticas actuales de vigilancia y proteger a las personas de las violaciones de su derecho a la privacidad.

44. Muchas delegaciones recordaron que cualquier limitación al derecho a la privacidad se debía basar en leyes accesibles, transparentes, claras, completas y no discriminatorias y se debía limitar a lo estrictamente necesario para salvaguardar el interés general en una sociedad democrática. Cualquier vigilancia estatal de los particulares debe ser proporcional y justa, debe estar en conformidad con las normas internacionales, se debe regir por el estado de derecho y debe estar sujeta a control. Debe haber garantías adecuadas y efectivas contra los abusos. Se señaló que la definición adecuada del límite de las injerencias arbitrarias o ilegales en el derecho a la privacidad sería uno de los retos de los próximos años. También se destacó que la vigilancia generalizada podía constituir una injerencia injustificada. Una delegación señaló que el artículo 17 del Pacto debía ser la base para el debate sobre los principios de la limitación —la legalidad y la arbitrariedad—, a los que se hacía referencia expresa en él.

45. Varias delegaciones señalaron que los Estados tenían preocupaciones legítimas de seguridad, incluida la amenaza del terrorismo y la ciberdelincuencia. Una delegación señaló que el uso de Internet para actividades delictivas y antisociales iba en aumento. Otra delegación señaló que la seguridad requería información, en particular con respecto a las comunicaciones digitales para combatir el terrorismo, mientras que otra afirmó que los gobiernos tenían la responsabilidad de proteger a las personas, y que la vigilancia de datos podía ser una medida eficaz y legítima con fines policiales. Había un amplio consenso, sin embargo, en que había que abordar las preocupaciones legítimas de seguridad en el marco del derecho internacional de los derechos humanos, incluido el derecho a la privacidad.

46. En respuesta a una pregunta sobre el intercambio de datos entre los organismos gubernamentales, la Sra. Nyst declaró que la misma supervisión y garantías procesales se debían aplicar a la información recogida directamente y a la obtenida mediante el intercambio de información. La Sra. Cleveland señaló que el Comité de Derechos Humanos había expresado preocupación al respecto[8]. El intercambio de datos entre diferentes organismos públicos de un país podía ser legítimo, siempre que la finalidad de la recogida y el uso de esos datos fuera la misma para cada uno de esos organismos, a fin de garantizar el cumplimiento de los principios de necesidad y proporcionalidad y, por tanto, no vulnerar el derecho a la privacidad.

47. Algunas delegaciones señalaron que Internet trascendía las fronteras geográficas tradicionales. Varias delegaciones recordaron que, como se afirmaba en el informe de la Alta Comisionada, el derecho de los derechos humanos se aplicaba cuando un Estado ejercía el poder fuera de su territorio, de manera que no pudiera eludir sus obligaciones internacionales de derechos humanos y sus propias leyes nacionales adoptando medidas fuera de su territorio que estarían prohibidas en él. Varias delegaciones recordaron que el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos debía leerse conjuntamente con el artículo 2 del Pacto, que establecía que las obligaciones de los Estados se aplicaban a todos los individuos que se encontraran en su territorio y estuvieran sujetos a su jurisdicción. Varias delegaciones señalaron que cualquier injerencia en el derecho a la privacidad debía cumplir los principios de legalidad, proporcionalidad y necesidad, independientemente de la nacionalidad o la ubicación de los individuos cuyas comunicaciones estuvieran intervenidas. Si bien muchas delegaciones subrayaron que la responsabilidad del Estado de proteger el derecho a la privacidad no terminaba en sus

[8] Véase la observación general Nº 16 (1988) del Comité de Derechos Humanos, sobre el derecho a la intimidad, párr. 10.

fronteras, algunas delegaciones expresaron su preocupación por la interpretación lata de la aplicación extraterritorial del Pacto y pidieron un debate a fondo sobre la cuestión de la extraterritorialidad con respecto al artículo 17.

48. La Sra. Nyst recordó que la mayoría de las operaciones de vigilancia se llevaban a cabo dentro de los Estados. En lo referente a la cuestión de las distinciones basadas en la ciudadanía con fines de vigilancia, señaló que no solo vulneraban el principio de no discriminación, sino que también era un enfoque muy anticuado y poco práctico, porque era difícil, si no imposible, conocer la nacionalidad del remitente de una comunicación electrónica. En cuanto a si el control de la infraestructura de telecomunicaciones podía calificarse de jurisdicción del Estado a los efectos del artículo 2 del Pacto, la Sra. Cleveland declaró que debido a que la comunicación digital trascendía la geografía, se necesitaba una concepción de la aplicación extraterritorial de las normas de derechos humanos para que los derechos humanos se pudieran proteger en línea y fuera de Internet. Señaló que había varios enfoques de la extraterritorialidad, la mayoría de los cuales se centraba en el concepto de jurisdicción fuera del territorio como algún tipo de control efectivo sobre una persona o un territorio, y que, bajo ese enfoque, se podía ver el ejercicio del control sobre la infraestructura de Internet como el ejercicio del control sobre un territorio que tenía efectos en los derechos de las personas, dondequiera que se encontraran.

49. Se señaló que la responsabilidad de respetar el derecho a la privacidad recaía en diversos actores. Algunas delegaciones subrayaron que la falta de supervisión efectiva había contribuido a la falta de rendición de cuentas por las intromisiones ilegítimas en el derecho a la privacidad, así como las deficiencias de depender de salvaguardias internas sin supervisión externa independiente. Se subrayó la necesidad de proteger los derechos de las víctimas. Una delegación observó que correspondía a cada Estado desarrollar mecanismos de supervisión nacional independiente y eficaz, para garantizar la correcta aplicación de las normas que regían la vigilancia electrónica. Una ONG declaró que había habido casos de vigilancia masiva con el fin de detener a defensores de los derechos humanos o identificar a los participantes en reuniones pacíficas, en los que los "sellos de caucho" de los tribunales habían sido fundamentales, o en los que se habían facilitado los datos personales recogidos por las empresas de telecomunicaciones mediante sistemas de verificación de los nombres a los organismos de inteligencia y de investigación sin ningún tipo de control judicial. Se subrayó la necesidad de regímenes de supervisión eficaces, prestando atención a los derechos de las víctimas a un recurso efectivo, incluida la participación de un poder judicial independiente e imparcial como salvaguardia fundamental.

50. En respuesta a las preguntas sobre las garantías procesales y los mecanismos de supervisión de que la ley fuera efectiva y se aplicara en la práctica, la Sra. Nyst explicó que una condición esencial para una supervisión mayor y más eficaz era el fin del secreto generalizado. Los gobiernos habían de ser más transparentes acerca de las actividades que tenían que realizar para proporcionar seguridad y no debían poner en peligro la infraestructura de una manera que estuviera más allá del control del público. Asimismo, señaló que todas las personas, especialmente los jueces y los abogados, debían tener una mejor comprensión de la forma en la que funcionaba la tecnología de Internet, lo cual las ayudaría a comprender mejor la manera en la que funcionaba la vigilancia. Subrayó la importancia de que toda medida de vigilancia estuviera autorizada por una autoridad judicial independiente y competente. Añadió que era esencial que se notificara a los particulares el hecho de que habían sido objeto de vigilancia, con el fin de que estuvieran en condiciones de obtener reparación. También señaló la necesidad de mecanismos más rigurosos de supervisión independiente, con conocimientos técnicos de la manera en la que funcionaba la vigilancia, para que se pudiera efectuar un examen de las consecuencias en los derechos humanos de la vigilancia por parte de los servicios de seguridad. Por último, señaló que un titular de un mandato de procedimientos especiales con conocimientos técnicos podría proporcionar orientación sobre las buenas prácticas y sobre lo que requería

el marco de los derechos humanos para garantizar la protección del derecho a la privacidad. La Sra. Botero agregó que no había uniformidad en las normas nacionales que regulaban la vigilancia y dijo que una buena práctica a nivel nacional era tener un órgano de expertos que se centrara específicamente en la tecnología y los derechos humanos en el contexto de la vigilancia. Señaló que la supervisión podía ser institucional, judicial, interinstitucional y por conducto de un defensor del pueblo, que las garantías procesales debían incluir la autorización judicial previa de las medidas de vigilancia y que el fundamento jurídico y los criterios para la decisión debían ser públicos.

51. En cuanto a una pregunta sobre la obligación de los Estados de proporcionar un recurso efectivo para las violaciones del derecho a la privacidad, la Sra. Cleveland señaló que si bien el artículo 2 del Pacto Internacional de Derechos Civiles y Políticos disponía la obligación de que los Estados concedieran un recurso efectivo, se trataba de una pregunta muy difícil, debido al secreto de las prácticas de vigilancia. Las personas a menudo no sabían que habían sido objeto de vigilancia y, por tanto, podrían carecer de fundamento porque no podían demostrar daños suficientes. Señaló que era necesario que los gobiernos fueran más transparentes acerca de los programas de vigilancia que estuvieran llevando a cabo, para permitir el escrutinio público. Señaló también que era importante que las personas recibieran una notificación específica de que habían sido objeto de vigilancia una vez finalizada esta. Señaló además que las normas de fundamentación debían ser lo suficientemente generosas como para permitir una impugnación significativa de los programas de vigilancia. En ese sentido, destacó que el Tribunal Europeo de Derechos Humanos requería una probabilidad suficiente, no una demostración, de daños reales. Señaló que los procesos judiciales secretos eran problemáticos, pero que algún tipo de prueba judicial era sin embargo importante. El principal desafío era hacer que esos procesos fueran lo más transparentes y eficaces posible.

52. Sobre la cuestión de si debería haber tribunales especializados para examinar las medidas de vigilancia, la Sra. Cleveland señaló que los Estados debían encontrar la manera de satisfacer los requisitos de transparencia y control democrático, permitiendo al mismo tiempo cierto grado de confidencialidad. Una buena opción era tener procedimientos especiales para tratar información clasificada, pero en los tribunales ordinarios. Sobre esa cuestión, la Sra. Nyst agregó que si bien era útil en cierto sentido contar con jueces especializados con conocimientos técnicos, era esencial que los tribunales permitieran que las partes estuvieran en igualdad de condiciones al impugnar la vigilancia. Era crucial, por tanto, que no hubiera tribunales secretos ni ningún procedimiento que permitiera interpretaciones secretas de las leyes. Cualquier tribunal que no permitiera la máxima transparencia y el escrutinio no permitiría que se corrigiera la asimetría de poder entre el individuo y el Estado y podría de hecho servir para legitimar las medidas de vigilancia ilegales.

C. Cuestiones específicas relativas a las entidades empresariales

53. Varias delegaciones plantearon el papel de las empresas privadas. Algunas delegaciones señalaron que las empresas habían sido objeto de presiones por los gobiernos, o habían sido obligadas a entregar datos. Otras señalaron que las empresas internacionales de Internet y tecnología de las telecomunicaciones habían estado desarrollando y ejecutando su propia capacidad de vigilancia o ayudando a los Estados en su vigilancia de las personas. El Sr. Nissim señaló que la tecnología utilizada por las empresas de telecomunicaciones era muy complicada, pero los gobiernos podían acceder a ella. Se refirió, por ejemplo, a la "inspección profunda de paquetes", que permitía que se examinara el contenido de las comunicaciones al transmitirse y, por lo tanto, permitía a los proveedores de servicios de Internet supervisar y analizar las comunicaciones de Internet de

los usuarios en tiempo real. El Sr. Nissim señaló que las empresas de telecomunicaciones utilizaban esta técnica para mejorar el servicio que prestaban a los clientes, pero que también podía ser utilizada por los gobiernos con fines de vigilancia, sin que la empresa de telecomunicaciones ni siquiera fuera consciente de lo que estaba sucediendo, como le había ocurrido a Orange en el curso de sus operaciones[9].

54. Muchas delegaciones pidieron que las empresas y los terceros fueran más transparentes y responsables en su conducta. Algunas delegaciones hicieron hincapié en que era necesaria una comprensión más profunda de la manera en la que los intermediarios y otras entidades empresariales podían cumplir su responsabilidad de respetar los derechos humanos, así como la determinación de la potestad reglamentaria que debía recaer en el sector público y privado. El Sr. Nissim confirmó que la transparencia era una cuestión clave para las empresas de telecomunicaciones que estaban bajo una fuerte presión para que fueran más transparentes. En ese sentido, señaló que el jefe ejecutivo de su empresa había firmado una carta de protección de datos, que comprometía a la empresa a proteger la seguridad de los datos personales de sus clientes; proporcionar el control a los clientes sobre sus propios datos personales y la forma en que se utilizaban; ser transparente en cuanto al tratamiento de los datos de sus clientes y usuarios en todas las etapas; y prestar apoyo a todos sus clientes y usuarios para ayudarlos a proteger su privacidad y gestionar sus datos de carácter personal. Señaló, sin embargo, que su empresa había sufrido dos violaciones de la privacidad desde que se firmó la carta e hizo hincapié en que la protección de los datos de la injerencia de los gobiernos era siempre un reto. Reiteró que era importante recordar que, aunque varias empresas de telecomunicaciones se habían comprometido a ser transparentes, la transparencia debía venir, en primer lugar, del Estado. Asimismo, recordó que las empresas de telecomunicaciones estaban obligadas por las leyes nacionales y, por tanto, que el marco jurídico en el que operaban variaba entre los diferentes países. Señaló la tendencia actual de las empresas a estudiar el marco jurídico en todos los países en los que operaban. Señaló que en algunos países, la legislación permitía la transparencia *ex post facto*, permitiendo a las empresas facilitar información sobre las solicitudes formuladas por los gobiernos, o los datos transmitidos a ellos, o permitiendo al Estado que hiciera lo propio. En otros Estados, ni la empresa ni el Estado podían ser transparentes acerca de las medidas que la empresa había tenido que compartir. Señaló que las empresas de telecomunicaciones trataban de proteger con los medios a su alcance el derecho internacional de los derechos humanos. Por ejemplo, señaló que durante la Primavera Árabe, un gobierno había solicitado a su empresa que enviara mensajes de texto a todos sus clientes de base. Tras una negativa inicial de la empresa, se envió a miembros de las fuerzas armadas para que reiteraran las demandas del gobierno. Su empresa envió el mensaje solicitado, junto con la firma de uno de los miembros de las fuerzas armadas presentes. Era un detalle pequeño, aunque importante, que permitió a la sociedad civil entender la situación.

55. El Sr. Nissim destacó la importancia de la participación de múltiples interesados. A fin de ilustrar esta cuestión, se refirió a otra situación que había afrontado su propia empresa, en la que el gobierno en cuestión había retirado las peticiones que había formulado a las empresas de telecomunicaciones, debido a varios factores, uno de ellos el hecho de que la sociedad civil había publicado esas peticiones. Señaló que apoyaría la elaboración de un instrumento jurídico a nivel internacional que se ocupara de las obligaciones de las entidades privadas en materia de protección del derecho a la privacidad frente a las medidas de vigilancia, y que las leyes modelo y las mejores prácticas serían también de gran ayuda para los gobiernos.

[9] Véase Human Rights Watch, "They know everything we do: telecom and Internet surveillance in Ethiopia" (marzo de 2014).

D. Camino a seguir

56. Muchas delegaciones subrayaron la necesidad de que prosiguiera la participación de múltiples interesados. Dijeron que la participación del Estado no era suficiente, sino que las entidades privadas, la sociedad civil, las comunidades científica y técnica, el sector empresarial, el mundo académico y los expertos en derechos humanos debían participar en los debates. También se destacó la necesidad de una mayor participación del Consejo de Derechos Humanos.

57. Varias delegaciones pidieron que los Estados revisaran sus procedimientos, prácticas y legislación relacionados con la vigilancia y la interceptación de las comunicaciones y la recogida de datos personales, con el fin de adaptarlos a las necesidades del siglo XXI y asegurarse de que estuvieran en plena conformidad con el derecho internacional de los derechos humanos. Otras pidieron un sistema internacional transparente con un marco internacional adecuado de gobernanza de Internet, que incluyera garantías adecuadas para proteger los datos personales. Una delegación pidió la elaboración de un código de conducta sobre esas cuestiones. Varias delegaciones y ONG pidieron al Consejo que estableciera un mandato para un relator especial sobre el derecho a la privacidad, ya que era esencial para llamar la atención de forma específica y sostenida sobre esas cuestiones.

V. Conclusiones

58. **Los participantes en la mesa redonda llegaron a la conclusión de que el cambio tecnológico podría plantear nuevos desafíos a la legislación vigente. En tales casos, los marcos jurídicos establecidos, incluido el derecho internacional de los derechos humanos, seguirían aplicándose, incluso si la aplicación de la ley se debía adaptar para hacer frente a la nueva realidad. En cuanto a la promoción y la protección del derecho a la privacidad, en particular en el contexto de la vigilancia interna y extraterritorial, el marco internacional de los derechos humanos era claro. Era necesaria, sin embargo, una mejor aplicación a nivel nacional de las normas internacionales relativas al derecho a la privacidad, mediante una legislación nacional adecuada y unas garantías y una supervisión más sólidas.**

59. **Los participantes en la mesa redonda señalaron que el desarrollo de salvaguardias legales contra las violaciones y una supervisión efectiva con la participación de todos los interesados eran esenciales. Se debe aumentar la participación y mejorar los recursos de tribunales independientes, imparciales y competentes para hacer frente a esos problemas complejos. Además, señalaron la necesidad de una mayor transparencia, con respecto a las políticas y la legislación de vigilancia y las interpretaciones legales y las resoluciones judiciales, en su caso. Se deben publicar las leyes y los reglamentos y la forma en que se interpretan y aplican. La potestad de los gobiernos para acceder a los datos relacionados con las comunicaciones se debe basar en un marco jurídico claro y transparente que incorpore los avances en la tecnología y esté en conformidad con el estado de derecho y las normas internacionales de derechos humanos.**

60. **Los participantes en la mesa redonda apoyaron las opiniones de los Estados, las organizaciones regionales y las ONG e hicieron hincapié en que la protección, la promoción y el respeto del derecho a la privacidad requería la participación sostenida de todas las partes interesadas, incluidos los gobiernos, la industria, la sociedad civil y las organizaciones internacionales. Pusieron de relieve la capacidad única de las Naciones Unidas de convocar a todos los interesados y estudiar los medios más eficaces para proteger el derecho a la privacidad e hicieron hincapié en que el Consejo de Derechos Humanos debía seguir tratando el tema, en particular mediante el**

examen periódico universal, con el aumento de la participación de la sociedad civil. El ACNUDH y el Alto Comisionado también deben seguir trabajando en la cuestión y los procedimientos especiales deben participar dentro de sus propios mandatos, según corresponda. También se debe tener en cuenta la necesidad de establecer un nuevo mandato de procedimientos especiales sobre el derecho a la privacidad, para examinar los desafíos actuales y la manera en que el derecho se debe conceptualizar en términos más generales.

61. **Por último, los participantes en la mesa redonda destacaron el papel fundamental desempeñado por las Naciones Unidas y otras organizaciones internacionales en la promoción de las normas jurídicas internacionales por las que se regían las actividades de las empresas privadas, en su intento de respetar los derechos humanos de sus clientes y demás usuarios. Las empresas recurren a las Naciones Unidas en busca de apoyo a la promoción de la incorporación de dichas normas en el derecho interno de los Estados Miembros. Al promover el marco internacional, las organizaciones internacionales también estaban apoyando a las empresas en el cumplimiento de su responsabilidad de respetar y proteger la privacidad de los usuarios, a medida que proseguían los avances tecnológicos. Se debería estudiar la cuestión de si se podría elaborar una ley modelo o un código de conducta.**