Naciones Unidas A/HRC/37/62

Asamblea General

Distr. general
25 de octubre de 2018
Español
Original: inglés

Consejo de Derechos Humanos
37º período de sesiones
26 de febrero a 23 de marzo de 2018
Tema 3 de la agenda
Promoción y protección de todos los derechos humanos, civiles, políticos, económicos, sociales y culturales, incluido el derecho al desarrollo

Informe del Relator Especial sobre el derecho a la privacidad* **

Nota de la Secretaría

En su informe, elaborado en cumplimiento de la resolución 28/16 del Consejo de Derechos Humanos, el Relator Especial sobre el derecho a la privacidad se centra en la labor realizada en los tres primeros años de su mandato, con particular atención a las cuestiones relacionadas con las actividades de vigilancia y la privacidad, y reflexiona sobre la función y los mandatos de los titulares de mandatos de los procedimientos especiales.

* El informe se presentó con retraso para incluir la información más actualizada posible.
** El anexo se reproduce tal como se recibió, en el idioma en que se presentó únicamente.

GE.18-17811 (S) 191118 211118
1817811

Informe del Relator Especial sobre el derecho a la privacidad

Índice

I. Introducción

1. El mandato del Relator Especial sobre el derecho a la privacidad comenzó el 1 de agosto de 2015. Conforme a lo dispuesto en la resolución 28/16 del Consejo de Derechos Humanos, el Relator Especial presenta un informe anual al Consejo y a la Asamblea General[1].

2. Este es el tercer informe que el Relator Especial presenta al Consejo y, por tanto, el último de su primer y actual mandato. Por ello, conviene aprovechar la oportunidad para repasar lo ocurrido en los tres últimos años, exponer de forma general las actividades realizadas, los logros alcanzados y las enseñanzas extraídas, y examinar el mandato presente y futuro.

3. Con ese propósito, el presente informe se ha dividido en cuatro partes. Tras la introducción, se describen las actividades, los logros y la labor futura del Relator Especial en cada una de las ocho esferas del mandato. En la tercera parte de este informe, el Relator Especial expone la fructífera labor realizada en relación con una de las prioridades del mandato: la protección de la privacidad y las actividades de vigilancia realizadas por los organismos del Estado o por cualesquiera otras instancias. El Relator también describe un proyecto de instrumento jurídico internacional sobre las actividades de vigilancia y formula diversas recomendaciones a fin de que sean tomadas en consideración. En la cuarta y última parte del informe, el Relator Especial aborda los términos del mandato y las aclaraciones y los refuerzos que requiere.

4. Desde el comienzo del mandato, el derecho a la privacidad se ha consagrado y tutelado en los planos internacional[2] y regional[3], así como en otros instrumentos de derechos humanos[4], y el Consejo ha reafirmado la importancia de la vida privada, en particular en su resolución 34/7. En esa resolución, el Consejo reconoció que el derecho a la privacidad podía 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 observó con preocupación que las violaciones o transgresiones del derecho a la privacidad podían 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. Ello se ajusta al enfoque que el Relator Especial adoptó sobre la personalidad en su informe al Consejo de 2016 (A/HRC/31/64).

[1] Véase www.ohchr.org/EN/Issues/Privacy/SR/Pages/AnnualReports.aspx.

[2] Véase la Declaración Universal de Derechos Humanos, art. 12; el Pacto Internacional de Derechos Civiles y Políticos, art. 17; la Convención sobre los Derechos del Niño, art.16, y la Convención Internacional sobre la Protección de los Derechos de Todos los Trabajadores Migratorios y de sus Familiares, art. 14. Véase también www.ohchr.org/EN/Issues/Privacy/SR/Pages/Internationalstandards.aspx.

[3] Véase el Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, art. 8, y la Convención Americana sobre Derechos Humanos, art. 11. Véase también www.ohchr.org/EN/Issues/Privacy/SR/Pages/Internationalstandards.aspx.

[4] Por ejemplo, véase la Declaración de El Cairo sobre Derechos Humanos en el Islam, art. 18; la Carta Árabe de Derechos Humanos, arts. 16 y 21; la Declaración de Principios sobre la Libertad de Expresión en África de la Comisión Africana de Derechos Humanos y de los Pueblos; la Carta Africana sobre los Derechos y el Bienestar del Niño, art. 10; la Declaración de Derechos Humanos de la Asociación de Naciones de Asia Sudoriental, art. 21; el Marco de Privacidad del Foro de Cooperación Económica Asia-Pacífico; el Convenio del Consejo de Europa para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal; el Protocolo Adicional del Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, en lo relativo a las autoridades de supervisión y los flujos transfronterizos de datos; la Recomendación núm. R(99)5 del Comité de Ministros de los Estados miembros del Consejo de Europa, sobre la protección de la privacidad en Internet; y la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

5. En el desempeño de su labor, el Relator Especial se guía por el marco jurídico internacional sobre el derecho a la privacidad y por las resoluciones pertinentes que el Consejo aprueba de forma periódica, incluida la antes mencionada.

II. Mandato del Relator Especial

6. Las actividades del Relator Especial suelen vincularse a más de una esfera de su mandato, por lo que se informa de ellas en los apartados correspondientes a varios ámbitos del mandato. El mandato figura en el apéndice 1, que se encuentra disponible en línea (véase la parte V).

A. Actividades del Relator Especial (2015 a 2017)

1. Recopilación de información y cuestiones de estudio pertinentes

7. En el primer párrafo del mandato se dispone que el Relator Especial reunirá información pertinente relativa al derecho a la privacidad y formulará recomendaciones para garantizar su promoción y protección, en particular en relación con los retos que plantean las nuevas tecnologías.

8. Para lograr ese primer objetivo, el Relator Especial ha establecido cinco líneas de acción temáticas. Además, ha realizado visitas oficiales a países y consultas, ha mantenido contactos con organizaciones no gubernamentales (ONG), ha organizado debates públicos sobre la privacidad, conferencias internacionales y actos de promoción, como la Semana de Concienciación sobre la Privacidad que anualmente celebran las Autoridades de la Privacidad de Asia y el Pacífico, y ha examinado asuntos que se señalaron a su atención y cartas de transmisión de denuncias, entre otros medios, para analizar las cuestiones pertinentes.

Líneas de acción temáticas

9. El Relator Especial esbozó su plan de trabajo para 2016 en los informes que presentó al Consejo y a la Asamblea General, e invitó a todas las partes interesadas a que se implicaran en los informes temáticos y en las llamadas a consultas previstos, todos ellos relacionados con las cinco líneas de acción temáticas.

10. Las cinco líneas de acción temáticas son: una mejor comprensión de la privacidad, seguridad y vigilancia, macrodatos y datos abiertos, datos sanitarios, y el uso de los datos personales por las empresas. Todas las líneas de acción temáticas abordan los retos que afronta la privacidad en la era digital y están interconectadas y secuenciadas, de modo que cada equipo de tareas pueda valerse de la labor realizada por los demás. Por ejemplo, el Equipo de Tareas sobre Macrodatos y Datos Abiertos facilita la labor de las líneas de acción temáticas sobre datos sanitarios y sobre el uso de los datos personales por las empresas. Cada equipo de tareas está coordinado por un presidente que ayuda al Relator Especial de forma voluntaria recabando investigaciones e información, señalando problemas y realizando las consultas más amplias posibles.

a) Seguridad y actividades de vigilancia

11. El Relator Especial creó el Foro Internacional de Supervisión de los Servicios de Inteligencia con objeto de que se determinaran las mejores prácticas en materia de salvaguardias para la vigilancia de Internet. Se trata de un encuentro anual de organismos nacionales y comisiones parlamentarias que se ocupan de supervisar las cuestiones relativas a la inteligencia nacional y extranjera en sus respectivos países. El Foro es una plataforma en la que se comparte información, se intercambian experiencias y se determinan las mejores prácticas a nivel internacional.

12. El Foro ha sido un éxito rotundo. El comité organizador renueva sus miembros de forma regular. En 2016, el Foro se celebró en Bucarest con el apoyo de las cuatro comisiones de supervisión del Parlamento rumano, y acogió a más de 60 delegados que representaban a 26 instituciones de 20 países diferentes. En 2017 se celebró en el

Parlamento belga con el respaldo de las autoridades de protección de datos de Bélgica, Luxemburgo y los Países Bajos, y en él participaron 80 delegados procedentes de 30 países. En 2018 está previsto que se celebre en Portugal durante el otoño. Las autoridades de supervisión de varios países asumen cada vez más el proceso como propio y hacen notar los problemas y las soluciones en la esfera de la supervisión de los servicios de inteligencia considerándolos una preocupación internacional colectiva y respondiendo a la necesidad latente de adoptar las mejores prácticas relevantes para la protección de la privacidad.

13. Es precisamente la intersección entre la privacidad, los intereses de la seguridad del Estado y las actividades de vigilancia en el ciberespacio lo que condujo a que en 2015, tras las revelaciones que desde junio de 2013 había venido realizando Edward Snowden, se creara el mandato del Relator Especial. El Relator Especial comparte las impresiones del Presidente del Grupo de Expertos Gubernamentales sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional, quien, en octubre de 2017 y respecto a la recomendación de fomentar la concienciación sobre la existencia de vínculos entre la paz y la seguridad internacionales, los derechos humanos y el desarrollo en cuanto atañe al entorno de la tecnología de la información y de las comunicaciones (TIC), señaló que los Estados debían considerar su compromiso con los derechos humanos y las libertades fundamentales, y el respeto y la protección debidos a esos derechos y libertades, al compartir las lecciones y prácticas relativas a la respuesta al uso de las TIC con fines terroristas y otros fines delictivos, con inclusión de la cooperación entre los Estados y entre estos y el sector privado, al prevenir y contrarrestar el empleo de las TIC por grupos terroristas y otros grupos extremistas para reclutar e incitar a la violencia y para financiar, planificar y preparar sus actividades, y al determinar los casos en que podrían ser necesarios trabajos adicionales. El Grupo de Expertos Gubernamentales formuló varias recomendaciones para impulsar la aplicación de las normas voluntarias y no vinculantes sobre el comportamiento responsable de los Estados presentadas en el informe de 2015 del Grupo de Expertos Gubernamentales (A/70/174), entre otras, que los Estados, para garantizar la utilización segura de las TIC, han de acatar las resoluciones del Consejo de Derechos Humanos 20/8 y 26/13, sobre la promoción, la protección y el disfrute de los derechos humanos en Internet, así como las resoluciones de la Asamblea General 68/167 y 69/166, sobre el derecho a la privacidad en la era digital, a fin de garantizar el pleno respeto de los derechos humanos, incluido el derecho a la libertad de expresión. El Grupo de Expertos Gubernamentales subrayó que los datos personales conservados, transmitidos o procesados mediante las TIC pueden afectar profundamente a la vida y a la seguridad. Los Estados deberían adoptar las medidas adecuadas para proteger los datos personales, incluso su confidencialidad, integridad, accesibilidad y autenticidad, respetando los instrumentos jurídicos internacionales pertinentes de derechos humanos.

14. El Relator Especial hace notar que el Grupo de Expertos Gubernamentales no ha logrado consensuar un informe final y señala que ahora es más necesario que nunca lograr una sinergia entre todos los agentes internacionales cuyos mandatos incluyan el uso de las TIC para el tratamiento de datos personales.

15. El Relator Especial defiende sin cesar que la paz informática depende de la voluntad y la capacidad de los Estados para lograr una sinergia entre los intereses de seguridad y la privacidad en el ciberespacio. Para evitar la guerra informática también deben contemplarse iniciativas que pongan freno a las actividades de vigilancia y a otras medidas invasivas de la privacidad en el ciberespacio. Con miras a seguir sondeando posibles medidas de esa índole, y en sinergia con el proyecto de Alternativas de Gestión de la Privacidad, la Propiedad y la Gobernanza de Internet (MAPPING), financiado por la Unión Europea[5], el

[5] Para el Foro Internacional de Supervisión de los Servicios de Inteligencia y otros eventos, como los dedicados a la privacidad, la personalidad y los flujos de información, el Relator Especial recibe apoyo logístico de la Universidad de Malta y de la Universidad de Groningen, y celebra actos conjuntos con el proyecto MAPPING, financiado por la Unión Europea. Desde 2014, el Relator Especial ha sido el coordinador científico general del proyecto MAPPING, que se ocupa de la gobernanza de Internet, la privacidad y la propiedad intelectual. En el marco de ese proyecto, que finalizó de forma oficial en febrero de 2018, el Relator Especial también fue personalmente responsable de las áreas de gobernanza de Internet y privacidad, que desarrolló el Instituto de Derecho Informático de la Universidad Leibniz de Hannover (Alemania).

Relator Especial ha analizado opciones para la elaboración de un proyecto de instrumento jurídico internacional sobre las actividades de vigilancia y la privacidad que refuerce la normativa existente y establezca mecanismos de protección frente a la violación masiva en todo el mundo del derecho a la privacidad de las personas.

16. Con el examen y la adopción en el seno de las Naciones Unidas de un instrumento jurídico sobre las actividades de vigilancia y la privacidad se podrían lograr dos objetivos principales a un tiempo al proporcionar a los Estados lo siguiente:

a) Una serie de principios y disposiciones de referencia que puedan incorporarse a la legislación nacional y que representen y hagan efectivos los principios supremos del derecho internacional de los derechos humanos, en particular el derecho a la privacidad, en la esfera de las actividades de vigilancia;

b) Diversas opciones, basadas en las mejores prácticas internacionales, para conciliar los intereses de seguridad y las inquietudes relativas a las actividades de vigilancia con la protección del derecho a la privacidad.

17. Es necesario contar con algún tipo de instrumento, ya sea de carácter indicativo, como una recomendación, o incluso, y sería más apropiado dada la práctica actual de los Estados, de carácter imperativo, en forma de tratado multilateral internacional. Si bien la labor del Relator Especial ha sido muy fructífera hasta la fecha, en particular si se consideran los problemas que conlleva su mandato, aún no ha alcanzado la madurez necesaria que permitiría al Consejo de Derechos Humanos asegurar que ese instrumento cuente con el apoyo unánime, o siquiera mayoritario, de los Estados. A pesar de la necesidad apremiante de ese instrumento jurídico, es preciso tener en cuenta los problemas de calendario.

b) Macrodatos y datos abiertos

18. El informe del Relator Especial sobre los macrodatos y los datos abiertos se presentó a la Asamblea General en octubre de 2017 a modo de análisis introductorio en el que se determinaban los asuntos principales (A/72/540). Las recomendaciones preliminares abordaban las siguientes esferas:

a) Gobernanza, regulación, investigación y consulta con las organizaciones de la sociedad civil;

b) Límites al uso de la información personal, de acuerdo con normas y principios internacionales, incluida una categoría de datos personales exentos;

c) Mecanismos de aplicación rigurosos;

d) Requisitos para un análisis riguroso, público y científico de la protección de la privacidad de los datos, incluida una evaluación del impacto sobre la privacidad;

e) Apoyo activo de los Gobiernos y las empresas a la creación y el uso de tecnologías que promuevan el derecho a la privacidad.

19. El proceso de consulta ya está en marcha. El 28 de abril de 2018 se convocó la presentación de propuestas y se ha programado una consulta pública para julio de 2018. La labor en curso abordará los siguientes temas:

a) Principios orientativos para la protección de la privacidad en el contexto de los macrodatos;

b) Consulta sobre el informe y los problemas de privacidad que plantean los macrodatos;

c) Facilitación de la investigación sobre la anonimización;

d) Respuesta a los procesos fallidos de anonimización.

c) Datos sanitarios

20. El Equipo de Tareas sobre Datos Sanitarios instituido por el Relator Especial sobre la privacidad está examinando diversas cuestiones bajo la dirección del Dr. Steve

Steffensen, Profesor Adjunto de la Facultad de Medicina de la Universidad de Texas (Estados Unidos de América). Está previsto que se realice una consulta pública al respecto en 2018, probablemente en los Estados Unidos.

21. Se invita a todos los agentes interesados, los Estados y otras partes, incluidas las ONG, a que contribuyan a la elaboración de orientaciones relativas a las mejores prácticas.

d) Utilización de datos personales por las empresas

22. Algunas empresas, incluidas las mayores corporaciones, dependen cada vez en mayor medida de la explotación (recopilación, tratamiento, reutilización y venta) de la información personal, y a menudo no garantizan una transparencia adecuada y el consentimiento informado de las personas concernidas[6]. Durante su visita oficial a los Estados Unidos en junio de 2017, el Relator Especial sondeó a las empresas sobre la forma en que respondían a las solicitudes de los Gobiernos relativas a los datos personales en su poder. La preocupación que al Relator Especial le suscitaban esas solicitudes condujeron a la presentación de un informe *amicus curiae* al Tribunal Supremo de los Estados Unidos en diciembre de 2017[7].

23. El Relator Especial también se reunió con varias corporaciones de los Estados Unidos en 2017 para analizar la utilización de datos personales en sus modelos de negocio. Este diálogo está ayudando a que el Equipo de Tareas sobre la Utilización de Datos Personales por las Empresas pueda iniciar oficialmente su labor en 2018.

e) Privacidad y personalidad

24. El reconocimiento por el Consejo de Derechos Humanos del derecho a la privacidad como un derecho esencial en una sociedad democrática está siendo investigado por el Equipo de Tareas sobre la Privacidad y la Personalidad, que preside Elizabeth Coombs (Australia). Para ello, el Equipo realiza consultas y examina las comunicaciones recibidas y la bibliografía existente[8]. Con miras a promover una mejor comprensión de la privacidad en la era digital, el Relator Especial ha convocado actos regionales de consulta pública sobre la privacidad, la personalidad y los flujos de información. La primera de esas consultas (países occidentales) se celebró en julio de 2016 en Nueva York; la segunda (Oriente Medio y África del Norte), en Túnez en mayo de 2017; la tercera (Asia), en septiembre de 2017 en Hong Kong (China), y la cuarta (América Latina) está previsto que se celebre en mayo de 2018.

25. Además, el Relator Especial ha realizado las siguientes labores:

a) Ha examinado resoluciones históricas, como la dictada por el Tribunal Supremo de la India en 2017 en la causa *Justice K.S. Puttaswamy (Retd.) and Another v. Union of India and Others*. En la sentencia, el Tribunal Supremo declaró que "la privacidad es la máxima expresión de la santidad de la persona. Es un bien tutelado constitucionalmente que afecta a la totalidad de los derechos fundamentales y permite que la persona goce de un espacio de elección y autodeterminación"[9];

b) Ha dado a conocer los efectos de la privación del derecho a la privacidad en las personas y en su desarrollo;

c) Ha estudiado el fenómeno de la violencia cibernética con especial atención al análisis comparativo de género y a los sectores vulnerables de la comunidad[10];

[6] Véase www.ohchr.org/Documents/Issues/DigitalAge/ConceptNote.pdf.

[7] *United States of America v. Microsoft Corporation*, causa núm. 17-2, presentada el 13 de diciembre de 2017. Véase www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018 AnnualReportAppendix6.pdf.

[8] Resolución 34/7 del Consejo de Derechos Humanos.

[9] Véase http://supremecourtofindia.nic.in/pdf/jud/ALL%20WP(C)%20No.494%20of %202012%20Right%20to%20Privacy.pdf.

[10] Hadeel al-Alosi, "Cyber-violence: digital abuse in the context of domestic violence", *University of New South Wales Law Journal*, vol. 40 (4), págs. 1573-1603.

d) Ha analizado la importancia de la privacidad para el desarrollo pleno de las personas y de las sociedades en las que viven y a las que contribuyen.

Visitas oficiales a los países

26. Las fechas y el calendario de las visitas oficiales a los países se negocian con los Estados miembros pertinentes. Los países se seleccionan en gran medida considerando las novedades en la esfera de la privacidad.

27. Entre 2016 y 2018 se han cursado las siguientes solicitudes de visita oficial a los países:

País	*Fecha de solicitud*
China	31 de marzo de 2016
República de Corea	31 de marzo de 2016
Sudáfrica	31 de marzo de 2016
Estados Unidos de América	20 de septiembre de 2016
Alemania	21 de octubre de 2016
India	21 de octubre de 2016
Reino Unido	21 de octubre de 2016
Francia	29 de noviembre de 2016
Argentina	20 de diciembre de 2017
Uruguay	8 de enero de 2018

28. Los retrasos en las visitas a los países suelen ser consecuencia de que los Gobiernos tardan en responder a las solicitudes de visita o no las responden, o a que sobrevienen circunstancias que hacen inapropiada la visita del Relator Especial en la fecha prevista. Las visitas forman parte integrante de la función de vigilancia del derecho a la privacidad que desempeña el Relator Especial. Por ello, en los programas de las reuniones se prevé la participación de las siguientes personas:

a) Autoridades gubernamentales, como los servicios de inteligencia, los organismos encargados de hacer cumplir la ley, los organismos reguladores o de supervisión, y los ministros ante los que respondan esas autoridades;

b) Representantes de la sociedad civil y otras partes interesadas, incluidos activistas, periodistas, personalidades del mundo académico y otros.

29. En los órdenes del día de las reuniones suelen figurar los temas siguientes:

a) Marcos constitucional, legal e institucional;

b) Macrodatos, actividades de vigilancia, amenazas a la privacidad y las cinco líneas de acción temáticas del Relator Especial, así como evaluaciones de los mecanismos para la supervisión de los servicios de inteligencia;

c) Inquietudes compartidas por el Relator Especial, los expertos y las organizaciones de la sociedad civil.

Visitas oficiosas a los países

30. El Relator Especial visita países con otros fines, por ejemplo para asistir a conferencias internacionales, y recaba información que pueda ser útil para sus líneas de acción temáticas. Por ejemplo, en los cinco meses previos al informe presentado en 2016 a la Asamblea General, el Relator Especial participó en múltiples actividades en 11 países tan diversos y geográficamente distantes como Alemania, Australia, Austria, Dinamarca, los

Estados Unidos, Francia, Italia, Letonia, Nueva Zelandia, los Países Bajos y Suiza. Esas actividades permitieron determinar esferas importantes para la promoción de la privacidad, entre otras la protección de la vida privada de los niños y los aspectos estructurales y organizativos de los organismos reguladores de la privacidad y los datos.

Consultas

31. El Relator Especial ha colaborado con la sociedad civil, los Gobiernos, los organismos encargados de hacer cumplir la ley, los servicios de inteligencia, las autoridades de protección de datos, las autoridades de supervisión de los servicios de inteligencia, el mundo académico, las empresas y otras partes interesadas en África, América (América del Norte, Centroamérica y América del Sur), Asia, Australasia y Europa. Solo en 2016 y 2017, el Relator Especial visitó más de 30 ciudades diferentes, algunas en Asia, África del Norte y Centroamérica, una cuarta parte en los Estados Unidos y más de la mitad en Europa, para realizar 26 actividades.

Formulación de recomendaciones para garantizar la promoción y la protección del derecho a la privacidad, en particular en relación con los problemas que plantean las nuevas tecnologías

32. La información que se recopila en las actividades señaladas ayuda al Relator Especial a formular recomendaciones en sus informes al Consejo de Derechos Humanos y a la Asamblea General.

Logros

33. Hasta la fecha se han presentado los informes temáticos siguientes:

- Enfoques preliminares para supervisar de una manera más favorable a la privacidad las actividades de vigilancia realizadas por los organismos del Estado, Consejo de Derechos Humanos, marzo de 2017 (A/HRC/34/60).
- Seguridad y vigilancia, Consejo de Derechos Humanos, marzo de 2017 (A/HRC/31/64).
- Informe provisional sobre la labor del Equipo de Tareas sobre Macrodatos y Datos Abiertos, Asamblea General, octubre de 2017 (A/72/540).
- Algunas opciones preliminares para la gobernanza de Internet destinadas a un instrumento jurídico internacional sobre las actividades de vigilancia realizadas por los organismos del Estado, Consejo de Derechos Humanos, marzo de 2018 (véase el presente informe y su apéndice 7, que puede consultarse en línea).

Avances en curso en las líneas de acción temáticas

34. El Relator Especial formuló unas orientaciones sobre los macrodatos que presentó a la Asamblea General en octubre de 2017 y que actualmente son objeto de consultas; y un proyecto de instrumento jurídico internacional sobre las actividades de vigilancia y la privacidad que aborda los problemas identificados.

35. El Relator Especial ha celebrado consultas públicas, entre otras la Conferencia sobre la Privacidad, la Personalidad y los Flujos de Información: Perspectivas en Asia sobre la Privacidad como Derecho Humano Global (2017).

36. El Equipo de Tareas sobre Datos Sanitarios ha comenzado su labor bajo la dirección del Relator Especial.

37. El Relator Especial recabó apoyo para el Equipo de Tareas sobre la Utilización de Datos Personales por las Empresas y presentó el informe *amicus curiae* correspondiente al Tribunal Supremo de los Estados Unidos en relación con la causa Microsoft.

Visitas oficiales a los países

38. El Relator Especial ha realizado dos visitas oficiales, una a los Estados Unidos (junio de 2017)[11], y otra a Francia (noviembre de 2017)[12]. Los informes se presentarán al Consejo de Derechos Humanos en marzo de 2019 con objeto de disponer de más tiempo para los intercambios de seguimiento con los Gobiernos interesados.

Consultas

39. Las consultas han logrado que jurisdicciones distintas y niveles y sectores de la comunidad diferentes cobren mayor conciencia de los problemas que afecten a la privacidad. Entre ellas se cuentan, por ejemplo, los eventos organizados por el Irish Council for Civil Liberties, la Japan Civil Liberties Union, la Japan Federation of Bar Associations y la Comisión de Derechos Humanos de Irlanda del Norte, así como las múltiples actividades celebradas en el Foro para la Gobernanza de Internet y en RightsCon.

Actividades y oportunidades futuras

40. El Relator Especial tiene intención de presentar los informes siguientes si el Consejo de Derechos Humanos renueva su mandato:

a) Al Consejo de Derechos Humanos:

i) "Enseñanzas extraídas para mejorar las salvaguardias y las vías de reparación en relación con la supervisión eficaz de las actividades de vigilancia realizadas por los organismos del Estado", marzo de 2019;

ii) "Proporcionalidad, necesidad y ley en las actividades de vigilancia realizadas por los organismos del Estado, el cumplimiento de la ley y los flujos transfronterizos de datos personales: eficacia y mejora de las salvaguardias y los recursos legales existentes", marzo de 2020;

iii) "Avances, retrocesos y otras dimensiones de la supervisión efectiva sobre las actividades de vigilancia realizadas por los organismos del Estado", marzo de 2021.

b) A la Asamblea General:

i) "Mejora de las salvaguardias y las vías de reparación en materia de privacidad y datos sanitarios", octubre de 2018;

ii) "Lucro y privacidad: la monetización de datos personales como modelo de negocio y las responsabilidades de las empresas", octubre de 2019;

iii) "Privacidad, personalidad y flujos de información: primera visión general del derecho global a la privacidad desde las perspectivas del tiempo, el lugar y el espacio", octubre de 2020;

iv) "El flujo transfronterizo de datos personales: empresa, cumplimiento de la ley y actividades de vigilancia", octubre de 2021.

41. El Relator Especial también podría informar, si el tiempo y los recursos lo permiten, sobre otras cuestiones relacionadas con el derecho a la privacidad: los macrodatos y los datos abiertos; los datos sanitarios; el uso de la información personal por las empresas; la vida privada de los niños y los jóvenes; las estrategias para afrontar los problemas relativos a la privacidad inherentes a las actividades de vigilancia; un enfoque de género sobre el derecho a la privacidad; las respuestas a las violaciones de la vida privada, por ejemplo a los procesos fallidos de anonimización de macrodatos; las quejas recibidas por el Relator Especial; las visitas oficiales a los países; las cuestiones que se estén examinando junto con los Estados (cartas de dominio público); y la privacidad en la era digital.

[11] Véase la declaración de final de la misión, que puede consultarse en www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/VisitUSA_EndStatementJune2017.docx.

[12] Las conclusiones preliminares pueden consultarse en www.ohchr.org/FR/NewsEvents/Pages/DisplayNews.aspx?NewsID=22410&LangID=F.

42. Las próximas visitas oficiales previstas para el Relator Especial tendrán como destino el Reino Unido de Gran Bretaña e Irlanda del Norte (junio de 2018) y Alemania (otoño de 2018).

43. El Relator Especial seguirá celebrando consultas sobre el derecho a la privacidad con instituciones públicas, particulares y organizaciones. Entre los eventos principales de 2018 cabe señalar la Conferencia del proyecto MAPPING celebrada los días 19 y 20 de enero en Roma; el acto de América Latina sobre la privacidad, la personalidad y los flujos de información, cuya celebración está prevista para mayo; y la consulta del Equipo de Tareas sobre Datos Sanitarios, y la consulta sobre macrodatos y datos abiertos, que se celebrarán en Australia en julio.

2. Solicitud y recepción de información, y respuesta a la información recibida

Consultas

44. El Relator Especial intercambió información con funcionarios, ministerios e instituciones de diversos países (a nivel nacional y subnacional); autoridades de protección de datos y privacidad; el Presidente del Grupo de Trabajo del Artículo 29, de la Unión Europea; el Presidente del Comité Consultivo del Consejo de Europa del Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal[13]; organizaciones de normalización, como la Unión Internacional de Telecomunicaciones y el Instituto de Ingenieros Electricistas y Electrónicos; organizaciones de la sociedad civil; misiones permanentes ante las Naciones Unidas y otras organizaciones internacionales con sede en Ginebra; otros titulares de mandatos de los procedimientos especiales; funcionarios de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (ACNUDH), investigadores, personalidades del mundo académico y órganos profesionales. El Relator también ha pronunciado discursos en calidad de orador principal y ha participado ampliamente en conferencias y reuniones de la sociedad civil.

45. El Relator Especial mantuvo contactos particularmente fructíferos con las autoridades de protección de datos y privacidad, que son uno de los principales grupos concernidos por su mandato. En la Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, celebrada en 2015, el Relator Especial solicitó la opinión de esas autoridades sobre su plan de diez puntos. En la Conferencia de 2016, el Relator Especial informó de que se habían logrado avances en relación con ese plan, y en la de 2017, celebrada en Hong Kong (China), intervino, participó en actos paralelos y celebró su tercer acto sobre "privacidad, personalidad y flujos de información", que complementó la Conferencia.

Correspondencia

46. El Relator Especial recibe correspondencia de diversas fuentes. Sin embargo, es difícil informar del número total de comunicaciones recibidas, ya que solo se registra y contabiliza la que se recibe a través del registro oficial del ACNUDH. Sea como fuere, el ACNUDH ha registrado en nombre del Relator Especial, desde el comienzo del mandato, la correspondencia siguiente.

47. Correspondencia registrada de 2015 a 2017[14]:

2015	*2016*	*2017*	*Total*
No se dispone de datos	3	47	50

48. No se dispone de datos desglosados por país o tema. Conviene señalar, sin embargo, que en 2017 la mayor parte de la correspondencia procedía de las misiones permanentes, las ONG y las organizaciones internacionales[15]. En esas cifras no se tienen en cuenta los

[13] Grupo de Protección de las Personas en lo que respecta al Tratamiento de Datos Personales, instituido en virtud del artículo 29 de la Directiva núm. 95/46/CE.

[14] Sin incluir los correos electrónicos remitidos a srprivacy@ohchr.org.

[15] Información recibida del ACNUDH, 19 de diciembre de 2017.

cientos, acaso miles, de otros mensajes recibidos en la dirección institucional de correo electrónico del Relator Especial (srprivacy@ohchr.org).

Logros

49. En octubre de 2015, la Conferencia Internacional de Autoridades de Protección de Datos y Privacidad aprobó una resolución sobre la cooperación con el Relator Especial[16].

50. El Relator Especial emitió comunicaciones conjuntas con otros titulares de mandatos sobre la situación en Egipto, España, Haití, Honduras y México.

51. El Relator Especial señaló las cuestiones emergentes, las acusaciones de violación del derecho a la privacidad y la posible invasión de la privacidad mediante medios tecnológicos, como el *software* de reconocimiento facial, y respondió a ellas.

Actividades y oportunidades futuras

52. El Relator Especial proseguirá sus actividades e insistirá en la colaboración con todas las partes interesadas (en particular para afrontar los problemas relativos a la seguridad y las actividades de vigilancia, incluida la ciberseguridad para los sistemas de información); elaborará material de orientación y recomendaciones sobre cuestiones emergentes con la colaboración de organizaciones de la sociedad civil y de otras partes interesadas; proporcionará asistencia técnica sobre los riesgos crecientes y diversos para el derecho a la privacidad en la era digital, y colaborará con otros titulares de mandatos de los procedimientos especiales para la protección de los derechos humanos.

3. Determinación de obstáculos, promoción de principios y formulación de recomendaciones

Dificultades para hacer efectivo el derecho a la privacidad

53. Una de las iniciativas más importantes del Relator Especial atañe a la esfera de la seguridad y las actividades de vigilancia, como no podía ser menos, puesto que se trata de la cuestión fundamental que impulsó la creación de su mandato por el Consejo de Derechos Humanos. Entre los obstáculos a la protección del derecho a la privacidad de las personas bajo vigilancia cabe señalar la carencia o la insuficiencia actuales de normas detalladas, procedimientos prácticos y mecanismos de supervisión adecuados que garanticen un control independiente, fiable y eficiente de las actividades de vigilancia, tanto a nivel nacional como internacional. En el anexo figura un resumen de los aspectos susceptibles de mejora que se han detectado en la esfera de la protección de la privacidad.

54. En cuanto a los macrodatos, debe tenerse en cuenta que ya no es necesario que la información sea "personal" para que identifique a un individuo[17]. Las posibilidades que brindan la tecnología y el análisis de datos permiten comprometer la privacidad solo disponiendo de información que "conduzca" a una persona y sus contactos.

55. En las líneas de acción temáticas se señalan los obstáculos contemporáneos a la protección y la promoción del derecho a la privacidad, entre otros la invasión de la privacidad por medios tecnológicos en el ámbito sanitario, el teléfono inteligente en el estrado de los testigos, la ciberviolencia, las diferencias entre comunidades en cuanto al grado de vulnerabilidad, los prejuicios por razón de género y otros prejuicios incorporados en algoritmos, el acceso por los Gobiernos a los datos del sector privado, y el reconocimiento facial y otras tecnologías.

[16] Véase https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Cooperation-with-UN-Special-Rapporteur-on-the-Right-to-Privacy.pdf.

[17] Graham Greenleaf, "Data protection: a necessary part of India's fundamental inalienable right of privacy – submission on the White Paper of the Committee of Experts on a Data Protection Framework for India", *University of New South Wales Law Research Paper*, núm. 6, enero de 2018. Se puede consultar en https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3102810.

Respuesta a los obstáculos y promoción de la privacidad

56. El Relator Especial ha emprendido en relación con las actividades de vigilancia una estrategia dirigida a consensuar medidas que fortalezcan el marco jurídico internacional y establezcan mecanismos adecuados de supervisión de esas actividades en todo el mundo.

57. El Relator Especial ha emitido comunicados oficiales en respuesta a cuestiones de actualidad relativas a la privacidad, a visitas oficiales a los países y a asuntos que requerían una respuesta coordinada con otros titulares de mandatos (véase el apéndice 3).

Promoción de principios y mejores prácticas

58. El Relator Especial se pronunció, por ejemplo, en las consultas públicas sobre proyectos de ley realizadas por los Gobiernos de la India y el Reino Unido y por el Parlamento de Australia[18]. El Relator Especial también remitió cartas en las que manifestaba su preocupación; algunas de ellas son aún confidenciales[19] y otras, como las dirigidas a los Gobiernos del Japón y México, son de dominio público.

Propuestas y recomendaciones al Consejo de Derechos Humanos

59. Las recomendaciones del Relator Especial sobre los macrodatos y los datos abiertos figuran en el apéndice 4 del presente informe.

60. Las recomendaciones preliminares formuladas por el Relator Especial tras su visita oficial a los Estados Unidos abarcan las actividades de vigilancia con fines de seguridad nacional (composición de la Junta de Supervisión de la Privacidad y las Libertades Civiles y artículo 702 de la Ley de Enmienda de 2008 de la Ley de Vigilancia y Adquisición de Inteligencia Extranjera de 1978); la vigilancia inteligente en entornos urbanos y las actividades de vigilancia al servicio de los organismos encargados de la aplicación de la ley; las situaciones a las que se aplica el Decreto 12333; los datos personales custodiados por empresas; la ampliación de la tutela otorgada por la Ley de Portabilidad y Responsabilidad del Seguro Médico de 1996, a todos los datos sanitarios; la gestión de la identidad de los trabajadores sexuales; la promoción de la comprensión del concepto de privacidad; y el fomento de las iniciativas estatales en favor de la privacidad. En lo que respecta a las actividades de vigilancia, el Relator Especial recomendó que se pusiera fin a toda discriminación en relación con las salvaguardias y los medios de defensa de la privacidad entre quienes son ciudadanos de los Estados Unidos o residentes en el país, por un lado, y quienes no lo son, por otro, y que el Congreso velara por que se promulgaran leyes nuevas que consideraran la vigilancia masiva una medida desproporcionada e innecesaria en una sociedad democrática.

61. El Relator Especial formuló también en sus informes anuales al Consejo de Derechos Humanos otras recomendaciones sobre la seguridad y las actividades de vigilancia.

Logros

62. El Relator Especial ha informado sobre obstáculos incipientes en sus informes anuales a la Asamblea General y al Consejo de Derechos Humanos (entre 2015 y 2017), así como en las quejas relativas a violaciones del derecho a la privacidad cometidas por Estados miembros.

63. El Relator Especial, para responder a esos obstáculos, ha abogado ante los Gobiernos contra las iniciativas y los programas que pudieran violar el derecho a la privacidad, ha constituido equipos de tareas sobre las líneas de acción temáticas, ha promovido “la privacidad desde el diseño” entre las empresas tecnológicas, ha elaborado un proyecto de instrumento jurídico sobre las actividades de vigilancia realizadas por los

[18] Propuesta presentada al Parlamento de Australia, Comisión Parlamentaria Mixta de Inteligencia y Seguridad, investigación sobre el proyecto de ley de enmienda de la legislación de seguridad nacional (espionaje e injerencia extranjera) de 2017, 24 de enero de 2018.

[19] A la espera de que venza el plazo de respuesta de 60 días.

organismos del Estado (véase la parte II), ha organizado consultas públicas, ha participado en eventos internacionales y ha publicado artículos.

64. El Relator Especial ha presentado las siguientes propuestas y recomendaciones, parte de las cuales se señalaron más arriba: un plan de acción de diez puntos (2015), las prioridades del mandato (líneas de acción temáticas) (2016), las recomendaciones preliminares que figuran en su declaración de final de la misión tras su visita oficial a los Estados Unidos (2017), y las recomendaciones sobre las actividades de vigilancia realizadas por los organismos del Estado (A/HRC/34/60) y sobre los macrodatos y los datos abiertos (2017) (A/72/540).

Actividades y oportunidades futuras

65. En marzo de 2019, el Relator Especial presentará su informe final sobre la visita oficial a los Estados Unidos, en el que hará hincapié en los mecanismos de supervisión para las situaciones en las que es de aplicación el Decreto 12333. El informe sobre su visita oficial a Francia se presentará en marzo de 2019.

66. El informe del Relator Especial sobre la privacidad y los datos sanitarios se presentará a la Asamblea General en octubre de 2018.

67. Las propuestas y recomendaciones finales del Relator Especial relativas a los macrodatos y los datos abiertos se darán a conocer después de que se celebren consultas internacionales a mediados de 2018.

4. Contribución a eventos internacionales para promover un enfoque sistemático y coherente del derecho a la privacidad

Actividades

68. El Relator Especial ha intervenido en numerosos eventos, incluso como orador principal, lo que le ha permitido trabar contacto con las partes interesadas principales y lograr una amplia cobertura mediática.

69. Entre las colaboraciones estratégicas que el titular del mandato mantiene en la actualidad se cuenta la cooperación con la Conferencia Internacional de Autoridades de Protección de Datos y Privacidad. Los días 19 y 20 de febrero de 2018, el Relator Especial presentó y moderó para el ACNUDH una de las sesiones del taller de expertos sobre el derecho a la privacidad en la era digital. Se presentará un informe sobre ese taller al Consejo de Derechos Humanos en su 39º período de sesiones (de conformidad con lo dispuesto en su resolución 34/7).

70. El Relator Especial está aplicando su plan de acción de diez puntos. Ese plan fue presentado al Consejo de Derechos Humanos en marzo de 2016 y abarca las siguientes iniciativas (véase A/HRC/31/64, párrs. 45 a 55):

a) Investigaciones y consultas sobre la protección del derecho a la privacidad en la era digital, en las que se subraye la necesidad de reforzar la protección del derecho a la privacidad de los niños y los jóvenes, así como la relación entre la privacidad y las cuestiones de género;

b) Labores encaminadas a promover la toma de conciencia, como la Semana de Concienciación sobre la Privacidad que organizan las Autoridades de Privacidad de Asia y el Pacífico, y otros eventos destinados a miembros de la comunidad, reguladores y organizaciones de los sectores público y privado;

c) Diálogo estructurado sobre la privacidad en la esfera de la seguridad y en las actividades de vigilancia, con la participación de las ONG, las autoridades de protección de datos y privacidad, las fuerzas del orden y los servicios de seguridad e inteligencia;

d) Enfoques integrales sobre las salvaguardias y los recursos legales, procedimentales y operativos, como el proyecto de instrumento jurídico y el informe *amicus curiae* ya citado;

e) Salvaguardias técnicas examinadas con la Asamblea General en octubre de 2017 y un compromiso continuado con el sector técnico para promover la elaboración de salvaguardias técnicas eficaces;

f) Diálogo con el sector empresarial, como se señaló más arriba;

g) Promoción de avances nacionales y regionales en los mecanismos de protección de la privacidad: el Relator Especial destaca el valor a nivel mundial de los avances nacionales y regionales en los mecanismos de protección de la privacidad[20]. El contacto con las autoridades de privacidad y protección de datos en todo el mundo facilita esa promoción;

h) Cooperación con la sociedad civil. El Relator Especial se reunió con 40 ONG durante sus seis primeros meses de mandato y sigue colaborando con ellas gracias a la labor que realizan los equipos de tareas temáticos y a las reuniones y los eventos públicos, como los relativos a la privacidad, la personalidad y los flujos de información;

i) El ciberespacio, la privacidad informática, el espionaje informático, la guerra informática y la paz informática: esas cuestiones se abordan en todos los informes del Relator Especial, como puede comprobarse en la labor desarrollada por la línea de acción temática sobre seguridad y vigilancia. También es importante la ciberviolencia contra los más vulnerables, incluida la violencia doméstica facilitada por dispositivos digitales, la difusión en línea no consensuada de imágenes íntimas y los riesgos para la privacidad de los niños pequeños;

j) Promoción del desarrollo del derecho internacional. En diciembre de 2017, el Relator Especial colaboró con la Escuela de Derecho Cibernético de la Facultad de Derecho de la Universidad de Harvard para presentar un informe *amicus curiae* al Tribunal Supremo de los Estados Unidos en la causa Microsoft, antes citada, considerando las posibles repercusiones de ese caso en el derecho internacional (véase el apéndice 6). El 24 de agosto de 2017, el Tribunal Supremo de la India falló por unanimidad en la importante causa de la jurisdicción constitucional *Justice K.S. Puttaswamy (Retd.) and Another v. Union of India and Others* y decretó que la privacidad es un derecho tutelado por la Constitución en la India. Este caso histórico puede impulsar la incoación de recursos de inconstitucionalidad contra otras leyes de la India[21] que atañan a cuestiones de género, recursos que el Relator Especial vigilaría de cerca.

Logros

71. Desde marzo de 2015, el Relator Especial ha pronunciado más de un centenar de discursos para promover la protección del derecho a la privacidad (véase el apéndice 5); creó un blog sobre la privacidad y la personalidad (www.privacyandpersonality.org); presentó un informe *amicus curiae* al Tribunal Supremo de los Estados Unidos; respondió a la consulta formulada por el Gobierno del Reino Unido en relación con la Ley de las Facultades de Investigación de 2016, y propuso una respuesta al fallo del Tribunal de Justicia de la Unión Europea; contribuyó a la investigación realizada por el Parlamento australiano sobre las repercusiones en los organismos encargados de hacer cumplir la ley de los avances en la tecnología de la información y las comunicaciones, así como a la investigación sobre la Ley de Enmienda de la Legislación de Seguridad Nacional (Espionaje e Injerencia Extranjera) de 2017, y colaboró con el Gobierno de la India en la elaboración del Libro Blanco sobre un marco para la protección de datos y con la Escuela de Derecho Cibernético de la Facultad de Derecho de la Universidad de Harvard.

Actividades y oportunidades futuras

72. El Relator Especial seguirá participando en eventos internacionales y organizándolos, por ejemplo, en las conferencias sobre privacidad, personalidad y flujos de

[20] Por ejemplo, la Ley de Intercambio de Datos (Sector Público) de Nueva Gales del Sur (Australia), de 2015, exige que el intercambio de datos se ajuste a lo dispuesto en la legislación reguladora de la privacidad.

[21] Véase https://inforrm.org/2017/09/04/case-law-india-puttaswamy-v-union-of-india-supreme-court-recognises-a-constitutional-right-to-privacy-in-a-landmark-judgment-hugh-tomlinson-qc/.

información, y seguirá examinando fallos judiciales históricos en materia de privacidad y personalidad, incluidas las cuestiones de género.

5. Concienciación sobre el derecho a la privacidad, incluidos los problemas y los remedios efectivos

73. El Relator Especial ha seguido desplegando iniciativas para fomentar la toma de conciencia sobre la importancia de promover y proteger el derecho a la privacidad, con especial énfasis en los problemas concretos que plantea la era digital, así como sobre la importancia de proporcionar a las personas cuyo derecho a la privacidad haya sido vulnerado un recurso efectivo acorde con las obligaciones internacionales de derechos humanos.

74. A mediados de 2016, la privacidad de uno de cada diez ciudadanos se vio comprometida en un Estado miembro cuando se hizo pública una base de datos con información supuestamente anonimizada sobre prestaciones sanitarias y farmacéuticas. Los facultativos y los pacientes pudieron ser reidentificados. El Relator Especial ha escrito en dos ocasiones al Estado miembro concernido. La correspondencia sigue siendo confidencial durante 60 días. Esta cuestión está estrechamente relacionada con el mandato de las líneas de acción temáticas sobre macrodatos y datos abiertos, y sobre datos sanitarios.

75. El 18 de mayo de 2017, el Relator Especial tomó la inusual medida de publicar en el sitio web del ACNUDH[22] una carta de transmisión de denuncia al Gobierno del Japón, y actualmente se encuentra a la espera de que el Gobierno lo invite a participar en los debates sobre las normas del derecho internacional de los derechos humanos.

76. El 19 de julio de 2017, el Relator Especial emitió junto con otros titulares de mandatos de los procedimientos especiales un comunicado conjunto en el que se instaba al Gobierno de México a llevar a cabo una investigación transparente, independiente e imparcial de las denuncias de vigilancia y control ilegal de defensores de los derechos humanos, activistas sociales y periodistas[23].

77. El Relator Especial remitió una carta a un Estado miembro en relación con la inexistencia de vías de reparación a disposición de una persona que había sufrido una invasión inaceptable de su privacidad. La correspondencia se ha publicado en el informe de comunicaciones de los procedimientos especiales[24].

Logros

78. El Relator Especial ha seguido señalando a la atención de los Estados deficiencias patentes en la gestión de la privacidad y ha velado por que las cuestiones pertinentes relativas a la privacidad sean de dominio público.

Actividades y oportunidades futuras

79. El Relator Especial solicitará reparaciones ajustadas a las obligaciones internacionales para las personas que denuncien violaciones de la privacidad, y seguirá trabajando junto con los Estados miembros y las ONG para identificar y dar voz a los denunciantes que no tengan acceso a recursos nacionales.

6. Integración de la perspectiva de género

Actividades

80. La labor temática sobre la privacidad, la personalidad y los flujos de información que realiza el Relator Especial se guía por la idea de que la privacidad es un derecho fundamental en sí mismo que permite hacer efectivo el derecho primordial y básico a desarrollar la personalidad de forma libre y sin trabas. Esa iniciativa se puso en marcha en

[22] Véase www.ohchr.org/Documents/Issues/Privacy/OL_JPN.pdf.

[23] Puede consultarse en https://www.ohchr.org/SP/NewsEvents/Pages/DisplayNews.aspx?NewsID=21892&LangID=S.

[24] Véase www.ohchr.org/EN/HRBodies/SP/Pages/CommunicationsreportsSP.aspx.

julio de 2016 en Nueva York con una ceremonia a la que asistieron 90 expertos, reguladores y representantes de empresas y organizaciones de la sociedad civil procedentes de cinco continentes.

81. La segunda consulta de ese tipo, celebrada para la región del Oriente Medio y África del Norte los días 25 y 26 de mayo de 2017 en Túnez, contó con el apoyo de las autoridades nacionales de protección de datos. El evento acogió a unos 70 participantes procedentes de Argelia, Egipto, Líbano, Marruecos, Qatar, la República Árabe Siria y Túnez. El encuentro dedicado a la perspectiva de género ayudó a comprender la experiencia particular de las mujeres y supuso una aportación relevante.

82. La tercera consulta se celebró los días 29 y 30 de septiembre de 2017 en Hong Kong (China), durante la Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, gracias a la cooperación del Grupo de Investigación sobre Seguridad, Tecnología y Privacidad Electrónica de la Universidad de Groningen (Países Bajos), el Departamento de Políticas y Gobernanza de la Información de la Universidad de Malta y el proyecto MAPPING. Digital Asia Hub, la Universidad de Hong Kong y la autoridad de privacidad de Hong Kong (China) fueron los socios y anfitriones locales. El evento estuvo dedicado a las novedades y tendencias en Asia e incluyó sesiones celebradas por separado sobre las tradiciones asiáticas sobre la privacidad y las actividades de vigilancia, la privacidad y su relación con otros derechos humanos en Asia, y género y privacidad en Asia.

83. La celebración de la cuarta consulta está prevista para el primer trimestre de 2018 y contará con una o varias sesiones dedicadas a las cuestiones de género.

84. Generó profunda inquietud un Estado miembro que no brindaba en su ordenamiento jurídico vías adecuadas de reparación a una mujer a la que un trabajador sanitario, empleando su teléfono personal, había fotografiado los genitales durante un tratamiento ginecológico, sin permiso y sin fines profesionales. Esa violación de la privacidad tuvo un efecto grave y causó estrés emocional, económico y familiar.

85. También es motivo de inquietud que procedimientos aparentemente legales para la notificación de trámites judiciales parezcan afectar a la privacidad de formas indeseadas y diferenciadas en cuestiones relativas a la identidad de género. El Relator Especial está examinando actualmente las inquietudes planteadas.

86. Durante la visita oficial del Relator Especial a los Estados Unidos, una persona trabajadora sexual planteó los efectos de la criminalización de la prostitución en el derecho a la privacidad de los trabajadores sexuales. Tal vez sea necesario revisar la regulación de las actividades de vigilancia realizadas por los agentes del orden en los casos relacionados con trabajadores sexuales[25].

87. En 2017 se dirigieron a los Estados varias comunicaciones elaboradas de forma conjunta con otros titulares de mandatos. Esas comunicaciones abordaban cuestiones de género[26] y el objeto y propósito de la resolución 34/7, en la que el Consejo de Derechos Humanos reconoció que la privacidad permitía el desarrollo de la personalidad.

88. El Relator Especial seguirá de cerca los casos subsecuentes al fallo dictado por el Tribunal Supremo de la India en la causa *Justice K.S. Puttaswamy (Retd.) and Another v. Union of India and Others*, que consideró la orientación sexual un atributo esencial de la privacidad.

89. El Relator Especial tiene sumo interés en examinar las repercusiones de la pérdida de la privacidad. Se ha redactado la propuesta, pero aún no se han determinado los recursos.

[25] La declaración de final de la misión puede consultarse en www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/VisitUSA_EndStatementJune2017.docx.

[26] Comunicaciones conjuntas dirigidas junto con otros titulares de mandatos a los Gobiernos de Haití (22 de septiembre de 2017), España (12 de octubre de 2017) y Egipto (31 de octubre de 2017).

Logros

90. El Relator Especial celebró consultas sobre la privacidad y el género en las líneas de acción temáticas; organizó encuentros sobre los aspectos del derecho a la privacidad relacionados con el género en el marco de las tres consultas sobre la privacidad, la personalidad y los flujos de información; promovió el intercambio de información entre las partes interesadas sobre los aspectos del derecho a la privacidad relacionados con el género, y planteó algunas cuestiones a los Estados miembros.

Actividades y oportunidades futuras

91. La cuarta consulta pública sobre la privacidad, la personalidad y los flujos de información, que se celebrará en el primer trimestre de 2018, incluirá un encuentro dedicado a los aspectos del derecho a la privacidad relacionados con el género. El Relator Especial seguirá analizando los fallos judiciales, como se indica más arriba, y llevará a cabo investigaciones sobre el género y el derecho a la privacidad.

7. Presentación de informes sobre presuntas violaciones, incluidos los retos que plantean las nuevas tecnologías

92. El Relator Especial ha seguido informando sobre las presuntas violaciones del derecho a la privacidad, incluidos los problemas que plantean las nuevas tecnologías, y ha señalado a la atención del Consejo de Derechos Humanos y del Alto Comisionado de las Naciones Unidas para los Derechos Humanos las situaciones que son motivo de especial inquietud.

Actividades

93. La pérdida grave de privacidad en un entorno sanitario descrita más arriba por el Relator Especial también es pertinente, ya que revela la necesidad de disponer de vías de reparación en esos casos[27]. Prosiguen las conversaciones con el Estado en cuestión.

Logros

94. El Relator Especial ha seguido señalando a la atención de los Estados miembros concernidos las denuncias de violación del derecho a la privacidad. El Relator Especial también ha promovido que los miembros del Consejo de Derechos Humanos tomen conciencia de las violaciones del artículo 12 de la Declaración Universal de Derechos Humanos y del artículo 17 del Pacto Internacional de Derechos Civiles y Políticos.

Actividades y oportunidades futuras

95. El Relator Especial seguirá informando sobre las presuntas violaciones del derecho a la privacidad y colaborando con los Estados miembros para abordar cuestiones que sean motivo de grave preocupación.

8. Informes anuales al Consejo de Derechos Humanos y a la Asamblea General

96. En cumplimiento de su mandato, el Relator Especial ha informado anualmente al Consejo de Derechos Humanos y a la Asamblea General.

Informes anuales al Consejo de Derechos Humanos

97. Este es el informe anual al Consejo de Derechos Humanos correspondiente a 2018. En él se describen las actividades del Relator Especial desde 2015, se da cuenta de su exitosa labor en favor de la protección del derecho a la privacidad y en relación con las actividades de vigilancia realizadas por los organismos del Estado, y se analiza el mandato establecido por el Consejo de Derechos Humanos.

[27] Las diversas comisiones de reforma legislativa del Estado han recomendado en ocho ocasiones diferentes durante el último decenio la aprobación de normas reglamentarias que determinen la responsabilidad en casos de intromisión grave en la vida privada.

98. El contenido de los dos informes previos remitidos al Consejo se ha descrito más arriba.

Informes anuales a la Asamblea General

99. En su informe anual de 2017 a la Asamblea General, el Relator Especial informó sobre la marcha de los trabajos realizados por las líneas de acción temáticas y presentó un informe provisional sobre los macrodatos y los datos abiertos. El Relator Especial presentó el proceso de consultas propuesto y se refirió a un caso de datos sanitarios anonimizados que se habían hecho públicos y podían reidentificarse. Esta cuestión se ha planteado al Estado concernido.

100. El contenido de los dos informes previos remitidos a la Asamblea General se ha descrito más arriba.

Actividades y oportunidades futuras

101. El Relator Especial seguirá presentando con arreglo a lo previsto informes anuales en los que se describirán las actividades realizadas y las cuestiones que hayan ido surgiendo, así como los informes de los equipos de tareas sobre las líneas de acción temáticas.

B. Labor del Relator Especial en la esfera prioritaria de la seguridad, las actividades de vigilancia y la privacidad

102. Como ha señalado el ACNUDH, en los últimos años el derecho a la privacidad ha atraído cada vez más la atención de la Asamblea General y de los mecanismos de derechos humanos, en particular las políticas y prácticas de vigilancia de numerosos Gobiernos en todo el mundo. En 2013, la Asamblea General aprobó la resolución 68/167, en la que expresó su profunda preocupación por los efectos negativos que pudieran tener la vigilancia y la interceptación de las comunicaciones para los derechos humanos. La Asamblea General afirmó que los derechos que asisten a las personas cuando están desconectadas de Internet también deben estar protegidos en línea, y exhortó a todos los Estados a que respetaran y protegieran el derecho a la privacidad en la comunicación digital. Los mecanismos de supervisión nacional, cuando los hay, suelen ser ineficientes, ya que no pueden asegurar la transparencia, cuando proceda, y la rendición de cuentas por las actividades de vigilancia de las comunicaciones y la interceptación y recopilación de datos personales que realice el Estado[28].

103. Los atentados terroristas perpetrados en Alemania, Bélgica, Francia y el Reino Unido crearon enfoques nacionales, y a veces internacionales, que priorizaron las respuestas de seguridad reactivas y de alto perfil sobre otras matizadas con cuidado y que tuvieran en cuenta los intereses de seguridad y la responsabilidad de proteger la privacidad de sus ciudadanos. En 2016 y 2017, Alemania, Bélgica, Francia, los Países Bajos y el Reino Unido, por citar solo algunos ejemplos, aprobaron leyes cuya eficacia, proporcionalidad y alcance variaban de forma notable. No existe ni una sola ley nacional en materia de actividades de vigilancia que se ajuste de forma cabal a las normas internacionales sobre el derecho a la privacidad y las respete.

104. A pesar del impulso generado por las revelaciones de Edward Snowden, la privacidad y la vigilancia son temas que pocos países están dispuestos a examinar. Sin embargo, la sociedad civil, el mundo académico y otras partes interesadas, incluido un número cada vez mayor de Gobiernos, han expresado un interés genuino en mantener un debate internacional adecuado y constructivo sobre la privacidad y las actividades de vigilancia.

105. El Relator Especial, en aplicación de los planes de acción presentados al Consejo de Derechos Humanos en su primer informe anual y en sus informes subsiguientes a la Asamblea General, ha tratado de responder a las preocupaciones expresadas por esos

[28] Véase www.ohchr.org/Documents/Issues/DigitalAge/ConceptNote.pdf.

agentes y de superar las diferencias que los separan mediante la convocatoria de diversos foros de intercambio y debate. El Relator ha abordado la cuestión de las actividades de vigilancia, que es básica para la privacidad, en colaboración con los Estados miembros, el proyecto MAPPING, financiado por la Unión Europea, y las organizaciones de la sociedad civil, con miras a evitar la duplicación de esfuerzos.

1. El camino hacia un instrumento jurídico internacional sobre las actividades de vigilancia y la privacidad

106. De las investigaciones y los debates mantenidos con los responsables de las políticas públicas, los organismos encargados de hacer cumplir la ley, los servicios de inteligencia y las organizaciones de la sociedad civil se desprende que un componente esencial de la solución para evitar convertirnos en una sociedad vigilada es establecer una norma que sea útil tanto en el derecho nacional como en el internacional.

107. El Relator Especial, consciente de que el derecho a la privacidad preocupa al Consejo de Derechos Humanos y a la Asamblea General, ha celebrado consultas con las partes interesadas en cooperación con el proyecto MAPPING. Esas consultas comenzaron en Washington D.C. en 2015. En 2016 se celebraron talleres en Malta y Nueva York. Las ideas, posiciones y sugerencias de los participantes se recogieron en un documento en forma de borrador de instrumento jurídico que podría utilizarse para muy diversos fines: como pauta orientativa o modelo para la elaboración de leyes nacionales reguladoras de las actividades de vigilancia, o como norma imperativa, por ejemplo a modo de tratado internacional multilateral.

108. Alentados por el apoyo prestado en el marco del Foro Internacional de Supervisión de los Servicios de Inteligencia, el Relator Especial y el proyecto MAPPING siguieron realizando consultas conjuntas sobre nuevas medidas jurídicas de derecho internacional encaminadas a mejorar la protección de la privacidad, frente al incremento de las actividades de vigilancia, y definir una base común para la supervisión eficaz de las prácticas de vigilancia en todo el mundo.

2. Desarrollo por un grupo de expertos

109. En marzo de 2017 se elaboró un proyecto revisado tras la reunión conjunta celebrada en Miami (Estados Unidos), en febrero de 2017 con el Módulo 4 del Grupo de Trabajo sobre la Gobernanza y la Vigilancia de Internet del proyecto MAPPING.

110. Durante 2017, el Relator Especial y el proyecto MAPPING, alentados por la acogida positiva dispensada a la idea de que se elaborara un instrumento jurídico, realizaron amplias consultas en todo el mundo. Un grupo de trabajo compuesto por unos 50 expertos que representaban a la sociedad civil, el proyecto MAPPING y las principales empresas de Internet analizaron el proyecto de instrumento jurídico y las actividades de vigilancia en mayo de 2017 en Malta, y en septiembre del mismo año en París. Tras la reunión de París, el 15 de septiembre de 2017, se celebró una consulta con funcionarios encargados de hacer cumplir la ley en la sede de la Organización Internacional de Policía Criminal (INTERPOL) en Lyon (Francia).

111. Las conclusiones extraídas en las reuniones de París y Lyon y el proyecto revisado de instrumento jurídico se distribuyeron en el Foro Internacional de Supervisión de los Servicios de Inteligencia, celebrado los días 20 y 21 de noviembre de 2017 en Bruselas. Las autoridades responsables de supervisar los servicios de inteligencia y a los profesionales de esos servicios tuvieron así la oportunidad de formular observaciones sobre el proyecto de instrumento jurídico y sobre la idea de constituir un grupo internacional de jueces y establecer un mandamiento judicial internacional de acceso a datos.

112. Esas consultas y otras medidas adicionales permitieron elaborar un texto suficientemente maduro para realizar una consulta pública más amplia durante 2018. El proyecto de instrumento jurídico se difundió en línea a principios de enero de 2018, medida que coincidió con la celebración en Roma entre los días 17 y 19 de enero de ese año del primer debate público.

113. El proyecto de instrumento jurídico sobre las actividades de vigilancia realizadas por los Gobiernos y la privacidad abarca, en su estadio de elaboración actual, los principios generales y los requisitos básicos en la materia, con inclusión de la aplicación, el alcance, los derechos, los sistemas y los datos, la colaboración entre múltiples interesados y los mecanismos para el acceso transfronterizo a los datos personales (véase el apéndice 7 del presente informe).

3. Opciones preliminares en el marco de la gobernanza de Internet para un instrumento jurídico internacional sobre las actividades de vigilancia realizadas por los organismos del Estado

114. La comunidad mundial debe sin duda adoptar medidas urgentes para velar por que se observen y apliquen eficazmente el artículo 12 de la Declaración Universal de Derechos Humanos y el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, y para ello se debe elaborar un marco jurídico claro y amplio sobre la privacidad y la vigilancia en el ciberespacio que haga efectiva la observancia nacional y transfronteriza de ese derecho. El derecho internacional de los derechos humanos, si bien establece normas universales del más alto nivel para la protección del derecho a la privacidad, carece del nivel de detalle suficiente para constituir el marco jurídico general básico que proporcione salvaguardias adecuadas en diversos contextos pertinentes, por ejemplo en las actividades nacionales y extraterritoriales de vigilancia. La mayoría de las regiones del mundo carecen de mecanismos de aplicación como los establecidos en los últimos 40 años en Europa y América del Norte. Un instrumento internacional incrementaría en muy gran medida el nivel de detalle, la claridad, la exhaustividad, las salvaguardias y las vías de reparación del marco jurídico internacional frente a las violaciones del derecho a la privacidad que a diario se comenten en el ciberespacio. La dificultad del asunto estriba en los detalles.

115. Muchos han elogiado el proyecto de instrumento jurídico por su visión y amplitud. Partes interesadas relevantes han alentado que se siga desarrollando. En la última consulta, organizada conjuntamente por el Relator Especial y el proyecto MAPPING y celebrada en Roma los días 18 y 19 de enero de 2018, se formularon varias observaciones importantes:

a) La labor realizada hasta la fecha ha permitido detectar problemas y definir normas y vías de amparo potenciales para las actividades de vigilancia realizadas en el ciberespacio. Esos trabajos deben hacerse públicos, de modo que se conviertan en un instrumento para la reflexión y el debate y proporcionen un proyecto modelo para los Estados miembros que actualmente consideren la posibilidad de adoptar leyes y establecer mecanismos institucionales dirigidos a garantizar la supervisión eficaz de las actividades de inteligencia;

b) El proyecto, en su estado actual, abarca numerosas cuestiones, y si bien mantenerlo tal cual presenta ventajas estratégicas y tácticas, reducirlo a dos o más instrumentos de menor tamaño y alcance podría facilitar su adopción;

c) Se necesitan estrategias que aborden el calendario necesario, a corto y largo plazo, para que el instrumento logre una aceptación amplia y sea viable;

d) El examen del proceso seguido para la adopción en el pasado de los instrumentos jurídicos del sistema de las Naciones Unidas revela lo siguiente:

i) Forjar el consenso internacional para un instrumento jurídico toma tiempo;

ii) Los Estados miembros individuales, los grupos regionales y las alianzas interregionales pueden desempeñar un papel fundamental en el proceso de adopción de un instrumento jurídico;

iii) Las organizaciones de la sociedad civil desempeñan un papel crucial en la promoción de la adopción de instrumentos jurídicos internacionales;

iv) Incluso las iniciativas más loables se enfrentan a una resistencia inicial.

e) Sin perjuicio de la labor que realice el Relator Especial, el proyecto MAPPING presentará a la Comisión Europea el instrumento jurídico en su estado actual como parte de su Documento de Políticas y Hoja de Ruta sobre la Gobernanza de Internet, a más tardar el 30 de abril de 2018 y, en última instancia, lo presentará al Parlamento

Europeo y al Consejo Europeo. La Unión Europea podría ser la agrupación regional más apropiada para apoyar con el tiempo un instrumento jurídico sobre las actividades de vigilancia y la privacidad a nivel mundial;

f) Los debates preliminares indican un mayor interés potencial en el proyecto de instrumento jurídico por parte de América Latina y África, aunque esta cuestión debe examinarse y desarrollarse más detenidamente;

g) Las partes interesadas que participaron en las consultas sucesivas indicaron lo siguiente en sus comentarios:

i) La comunidad regional y mundial de organismos encargados de hacer cumplir la ley, incluidas la Agencia de la Unión Europea para la Cooperación Policial e INTERPOL, han mostrado un gran interés en muchas de las disposiciones del proyecto de instrumento jurídico, aunque también han señalado que se necesitaría un tiempo considerable (entre dos y tres años) para celebrar consultas más detalladas en sus comunidades;

ii) Las federaciones de colegios de abogados y los abogados defensores en casos de violación de la privacidad de activistas apoyan firmemente el proyecto de instrumento jurídico, incluidos los mecanismos de aplicación propuestos, como el establecimiento de un mandamiento internacional de acceso a datos;

iii) La comunidad empresarial muestra un gran interés en el proyecto de instrumento jurídico, en particular porque recoge los principios respaldados públicamente por la coalición Reform Government Surveillance[29];

iv) Las comunidades de inteligencia señalan que algunos países cuentan con una legislación avanzada que se ajusta en un 90 % al proyecto de instrumento jurídico en su estado actual. Es necesario seguir trabajando en la definición de la vigilancia selectiva y la aplicación limitada de la vigilancia masiva, de modo que resulten más prácticas y apropiadas;

v) Las preocupaciones de la sociedad civil se han centrado en la oportunidad del proceso y en el riesgo de que algunos Estados se apropien del texto para socavar sus salvaguardias y de su formulación concreta;

vi) La región europea está a la espera del resultado del examen de algunos asuntos por el Tribunal de Justicia de la Unión Europea y el Tribunal Europeo de Derechos Humanos, previsto para finales de 2018 o para 2019. Esas resoluciones pueden fomentar el interés de las agrupaciones europeas en un proyecto de instrumento jurídico, pero esas y otras consideraciones están actualmente frenando que se avance en la consecución de un progreso consensuado. La situación podría no mejorar antes de 2019 o 2021.

4. Recomendaciones específicas en relación con las actividades de vigilancia

116. El Consejo de Derechos Humanos debería examinar el apéndice 7 para determinar los problemas y arbitrar algunas soluciones cuya inclusión en un futuro instrumento jurídico internacional sobre la privacidad y la vigilancia podría finalmente examinarse.

117. Los Estados miembros interesados en un instrumento jurídico que promueva de forma sustancial recursos y soluciones similares a los que figuran en el apéndice 7 deben ponerse en contacto con el Relator Especial para seguir examinando la manera de promover esos principios en los planos nacional, regional e internacional.

118. Considerando las cuestiones de calendario antes señaladas, el Relator Especial propone presentar al Consejo de Derechos Humanos, si procede y es oportuno, un informe con nuevas recomendaciones en marzo de 2021.

[29] Véase www.reformgovernmentsurveillance.com.

C. Capacidad del Relator Especial para presentar comunicaciones individuales

119. David Weissbrodt relata la experiencia del primer Relator Especial temático (sobre ejecuciones sumarias o arbitrarias) al solicitar la atención de un Estado en relación con un caso. El Gobierno pertinente respondió a la comunicación del Relator Especial cuestionando la capacidad de este para realizar esa solicitud[30].

120. El Relator Especial sobre las ejecuciones sumarias o arbitrarias comunicó por escrito a la Comisión de Derechos Humanos que la cuestión merecía un examen más detenido y que agradecería recibir la orientación que la Comisión pudiera ofrecer al respecto[31]. A ese respecto, la Comisión prorrogó el mandato del Relator Especial sobre las ejecuciones sumarias o arbitrarias en sus períodos de sesiones anuales subsiguientes y además concluyó, como señaló la delegación de Noruega, que esos casos estaban comprendidos en el mandato del Relator Especial y debían incluirse en los informes ulteriores (Noruega fue el principal patrocinador de la resolución pertinente)[32].

121. El Relator Especial se siente en buena compañía ya que en 2017, y en dos ocasiones diferentes, se cuestionó su capacidad para señalar asuntos a la atención de los Estados. El envío de comunicaciones a los Estados miembros y a otras partes interesadas es parte integral de las actividades básicas de todos los titulares de mandatos de los procedimientos especiales. Este procedimiento bien documentado y regulado permite a todos los titulares de mandatos intervenir directamente con los Gobiernos y otras partes interesadas en relación con las denuncias de violaciones de los derechos humanos incluidas en sus mandatos mediante cartas, por ejemplo llamamientos urgentes y cartas de denuncia[33].

122. La decisión del Relator Especial de intervenir en el asunto de la toma de una fotografía no autorizada (véase párr. 84 más arriba) se ajustaba a la resolución del Consejo de Derechos Humanos por la que se establecía el mandato, en la que se instaba explícitamente a los Estados a que respondieran con prontitud a los llamamientos urgentes del titular del mandato y a otras comunicaciones.

III. Conclusiones

123. **El Relator Especial ha utilizado los medios de que normalmente se valen otros Relatores Especiales para promover y proteger la privacidad, incluidos los llamamientos urgentes y las cartas de denuncia dirigidas a los Estados, el seguimiento de las denuncias individuales, la participación en conferencias y la realización de visitas oficiales y oficiosas a los países.**

124. **El Relator Especial también ha desarrollado varios medios innovadores para cumplir su mandato, entre otros el Foro Internacional de Supervisión de los Servicios de Inteligencia, que se celebra anualmente, los eventos regionales semestrales sobre la privacidad, la personalidad y los flujos de información (ya celebrados en América del Norte, Oriente Medio y Norte de África, y Asia, cuya próxima edición se celebrará en América Latina), y los equipos de tareas de las líneas de acción temáticas sobre Macrodatos y Datos Abiertos, sobre Datos Sanitarios y sobre Privacidad y Personalidad, con el objetivo de proporcionar un enfoque global más amplio sobre numerosas cuestiones relacionadas con la privacidad.**

125. **Reconociendo la gravedad de la amenaza que las actividades de vigilancia suponen para el disfrute del derecho a la privacidad, el Relator Especial ha codirigido los esfuerzos internacionales encaminados a elaborar un marco jurídico internacional**

[30] David Weissbrodt, “The three ‘Theme’ Special Rapporteurs of the UN Commission on Human Rights”, *American Journal of International Law*, vol. 80, núm. 3 (julio de 1986), págs. 685 a 699.

[31] E/CN.4/1986/21, pág. 100.

[32] Resolución 1986/36 del Consejo Económico y Social.

[33] Respecto a los procedimientos especiales del Consejo de Derechos Humanos, véase https://www.ohchr.org/SP/HRBodies/SP/Pages/Welcomepage.aspx.

amplio que regule la vigilancia en el ciberespacio, lo que también mejoraría las perspectivas de lograr la paz informática.

126. **Los procedimientos especiales constituyen un mecanismo importante del que se vale el Consejo de Derechos Humanos para que se elaboren y apliquen normas de derechos humanos[34]. Continuar elaborando normas internacionales sobre las actividades de vigilancia realizadas por los organismos del Estado permitirá a la comunidad internacional orientar y evaluar el uso de esa tecnología y de esas prácticas. Las normas relativas a las buenas y mejores prácticas se examinan de forma periódica en el Foro Internacional de Supervisión de los Servicios de Inteligencia.**

127. **El Relator Especial considera que un instrumento jurídico que regule las actividades de vigilancia en el ciberespacio y que complemente otros instrumentos en vigor sobre el derecho informático, como el Convenio sobre la Ciberdelincuencia del Consejo de Europa, podría proporcionar garantías concretas para la privacidad en Internet (A/HRC/34/60 y A/72/540), al tiempo que resolvería problemas de larga data, como la jurisdicción en el ciberespacio. Si bien la labor realizada hasta la fecha ha sido muy satisfactoria y alentadora, el respaldo a la forma y el contenido actuales del instrumento jurídico no es aún suficientemente homogéneo para que pueda recomendarse que el documento, en su forma actual, sea examinado de inmediato por el Consejo de Derechos Humanos. Sin embargo, con un esfuerzo constante y tiempo, ese instrumento viable podría presentarse al Consejo en un futuro relativamente cercano, posiblemente incluso antes de 2021.**

128. **Los titulares de mandatos de los procedimientos especiales son expertos independientes y constituyen un importante mecanismo para la protección de los derechos humanos. Los Estados miembros deben aceptar sus comunicaciones e investigaciones y cooperar plenamente con ellas, y deben abstenerse de cuestionar la legitimidad de sus críticas constructivas.**

IV. Recomendaciones al Consejo de Derechos Humanos

129. **El Consejo de Derechos Humanos debería tomar nota de los logros del Relator Especial durante su mandato a través de las líneas de acción temáticas, de la coherencia de esos logros con el plan que figura en su primer informe al Consejo, de las próximas medidas, en particular la propuesta de incorporar un tema adicional sobre la vida privada de los niños, y del calendario previsto para la presentación de los informes subsiguientes en el marco de las líneas de acción temáticas.**

130. **El Consejo debería tomar nota de los avances hacia la consecución de normas internacionales que regulen las actividades de vigilancia realizadas por los organismos del Estado, la creación, innovadora y satisfactoria, del Foro Internacional de Supervisión de los Servicios de Inteligencia, y la voluntad de elaborar a medio plazo un instrumento que las Naciones Unidas puedan examinar con vistas a que finalmente los Estados miembros y otras partes interesadas lo desarrollen.**

131. **El Consejo debería recomendar a la Asamblea General que se aplique un impulso renovado a todas las iniciativas de las Naciones Unidas encaminadas a analizar la intersección entre la privacidad, la seguridad y el comportamiento de los Estados en el ciberespacio, en sinergia con el Relator Especial sobre la privacidad, en un intento decidido de elaborar un marco jurídico más amplio para Internet.**

[34] Weissbrodt, “The three ‘Theme’ Special Rapporteurs”.

V. Guía de los documentos de apoyo

132. Por limitación de espacio, los siguientes documentos se han publicado en el sitio web del Relator Especial:

- Apéndice 1: Mandato del Relator Especial sobre el derecho a la privacidad

  http://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix1.docx

- Apéndice 2: Graham Greenleaf, Global Data Privacy Laws 2017: 120 National Data Privacy Laws, including Indonesia and Turkey

  http://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix2.docx

- Apéndice 3: Comunicaciones del Relator Especial sobre el derecho a la privacidad

  http://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix3.docx

- Apéndice 4: Informe provisional y recomendaciones preliminares del Equipo de Tareas sobre los Macrodatos y los Datos Abiertos

  http://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix4.docx

- Apéndice 5: Participación en eventos internacionales entre 2015 y 2017

  http://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix5.docx

- Apéndice 6: Informe *amicus curiae* al Tribunal Supremo de los Estados Unidos en relación con la causa *United States of America v. Microsoft Corporation*

  http://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix6.pdf

- Apéndice 7: Proyecto de instrumento jurídico sobre las actividades de vigilancia realizadas por los organismos del Estado

  http://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix7.docx

- Apéndice 8: Agradecimientos

  http://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2018AnnualReportAppendix8.docx

Anexo

[Inglés únicamente]

Paper presented at Expert workshop on the right to privacy in the digital age

Office of the High Commissioner for Human Rights

Geneva, 19–20 February 2018

1. Privacy is a fundamental human right recognized as such under international law. It is also a universal right, one which should be enjoyed everywhere by everybody, as such it should be respected everywhere by everybody, by States as well as by non-State actors, irrespective of the ethnicity, nationality, gender, religious, philosophical or political beliefs of any given individual or any other status. The recognition of the universal right to privacy is part of the set of fundamental norms established in the development of human rights law since World War II.

2. Due to its complexity, the right to privacy requires a comprehensive legal framework in order to operationalize it in a number of different contexts. These contexts may be as diverse as medical and health, insurance, statistics, national security, finance, police, social security, education and many others. Each context brings with it the need of a detailed and constantly up-dated understanding of how privacy could be threatened within that particular context and an identification of safeguards that protect it, and remedies available to citizens which may be specific to that context. The devil, literally, is in the detail, and privacy requires very detailed rules which spell out the level and modes of protection that privacy may be accorded in a particular context as well as the remedies that a citizen may resort to if his or her privacy is breached in that context. The importance of this level of detail is even greater in the case of privacy since there exists no universally accepted definition of privacy. In other words, people across the world have agreed that the right to privacy exists and that everybody is entitled to such a right but they have not spelt out precisely what the right is or what it entitles a person to in a wide variety of circumstances. This fact has both advantages and disadvantages: too narrow a definition of privacy would restrict its ability to be protected as circumstances and privacy-threats change and also as we develop our understanding of what constitutes privacy-infringing behaviour in a number of changing or new contexts.

3. The rules and remedies provided for at national law come together with those established under international law to constitute the international legal framework available for the protection of privacy. Those at the national level are most often to be found in an amalgam of principal and subsidiary legislation complemented by the case law of that particular country. The courts of all countries and especially those with constitutional competences interpret the extent — and occasionally the limits — of the right to privacy in accordance with their understanding of that country's constitution, the national law on privacy — if it exists — as well as, often enough, the precepts of international law on the subject. Very importantly, over the past forty years we have witnessed a huge growth in the impact of international law on national law in the sphere of privacy protection. We have seen the concerted development of international law at the regional level, most notably in Europe, which has then guided the development of national law and practices in diverse contexts where privacy may be threatened.

4. Moreover, privacy is not an absolute right. It is a qualified right. There exist a small number of very special occasions when limitations to the right to privacy may be introduced subject to a number of special measures which are normally best spelt out under international law as well as necessarily having a clear legal basis in domestic law. Some of these will be explored below in the context of security. The way that the right to privacy is

qualified needs to be spelt out in great detail in a given context. If limitations to the right to privacy are not adequately defined the gaps in privacy protection will increase.

5. An additional but essential overall consideration is that constantly developing technologies pose important challenges for the protection of privacy: these technologies may reveal the most intimate behaviour, wishes, preferences and indeed the very thoughts of individuals in ways that previously were not possible. Smartphones, credit cards and the Internet are three good examples of the types of technology that bring significant new challenges to the protection of privacy.

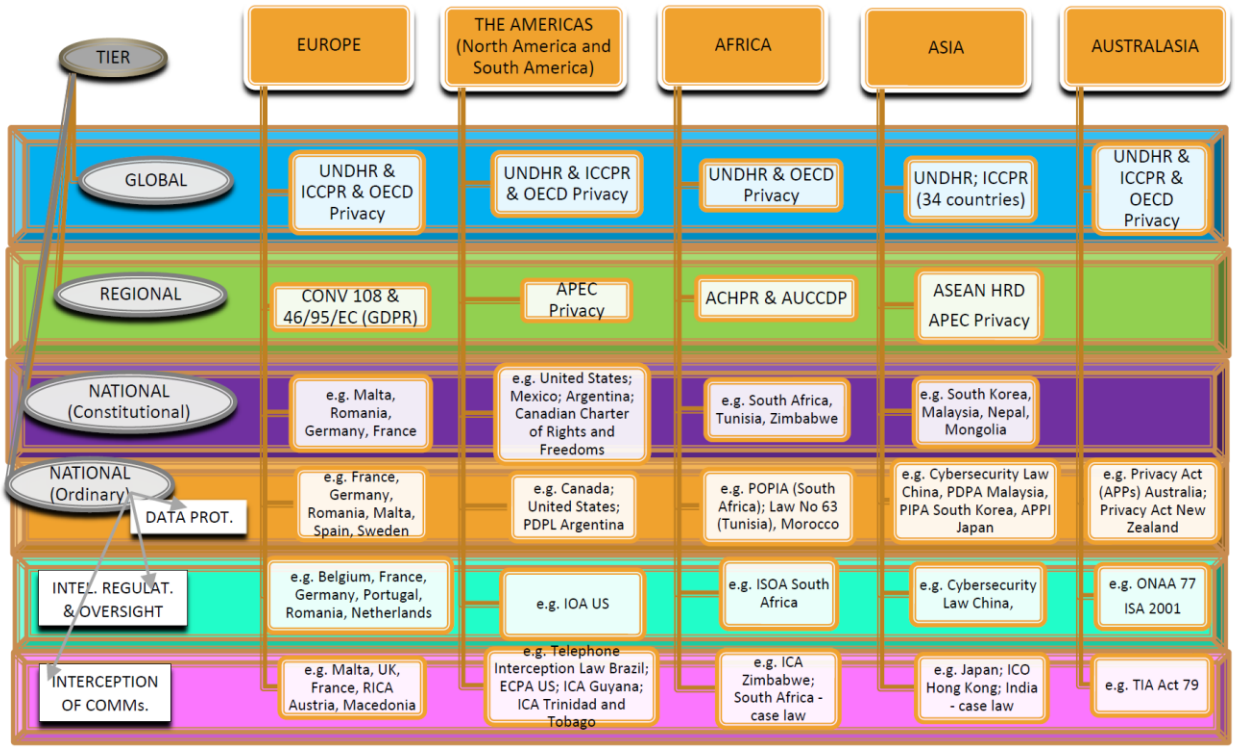
6. When dealing with technologies such as the Internet it is simplistic and naïve to be content with a statement that "whatever is protected off-line is protected on-line". That is a hopelessly inadequate approach to the protection of privacy in 2018. International law such as Art. 12 UDHR and Art 17 ICPPR only provides an answer to the question "Why?" as in "Why should we protect privacy" i.e. because we have agreed that it is a universal fundamental human right. They however do not provide answers to the questions: When? Which? What? How? Who? When should privacy be protected? How should privacy be protected? Which are the privacy-relevant safeguards to be created in a particular context? Which new contexts pose the greatest risks to privacy? What should be done to protect privacy in given circumstances? Which are the remedies most appropriate and possible in those cases where, despite all the safeguards provided, a breach of privacy still occurs? Who has special duties and obligations in the case of privacy protection, in which circumstances, what measures are the minimum to discharge these obligations and how should such persons be held accountable? The answers to these and other questions can only be found if the international and national legal framework is detailed enough.

7. Over the past fifty years some countries and some inter-governmental organizations have taken the initiative to develop their legal framework with respect to privacy but others have not. As a consequence, in 2018 more than a third of United Nations Member States have no privacy laws at all[1] while most of the other 125 states have laws which cover some of the contexts where privacy may be threatened but not all. Some important threats to privacy especially those arising in the context of national security, intelligence and surveillance are inadequately regulated in most countries of the world. International law, especially in the form of some regional initiatives, helps provide a level of co-ordinated response to some privacy threats for some countries but these remain, at best, a significant minority. The result is a patchwork quilt, in many places crocheted in stitches which are far too open to keep in the warmth and which, in any case, is not large enough to cover all of the bed. This patchwork quilt can in no way be characterized as a comprehensive and sufficiently detailed legal framework through which persons anywhere and everywhere can enjoy the universal right to privacy. It is the duty of the Special Rapporteur on the right to privacy, in conformity with his mandate, to identify the lack of a comprehensive, detailed and universal legal framework as a serious obstacle to the protection of the right to privacy world-wide. The rest of this paper, for reasons of time and space, mostly focuses on the lack of an adequate legal framework in two often-related contexts: national security and the prevention, detection, investigation and prosecution of crime but this is not to say that all other contexts are well served by the international legal framework.

The current international legal framework

8. The diagram below attempts to sketch out the international legal framework for the protection of privacy which exists so far:

[1] Though this does not exclude the possibility that their constitutional courts could be seized of privacy-related matters.



9. The diagram above is intended primarily to illustrate the tiered structure of the international legal framework but limitations of space do not permit one to clearly see that the tiers in Asia and Africa contain many more gaps and vacant spaces than those in Europe and North America. These gaps are however summarized in the overview text below.

Gaps in protection from government-led surveillance.

10. The surveillance of citizen behaviour on the internet can be broadly categorized into two main types: Government-led surveillance, and, surveillance or monitoring of citizens behaviour by private corporations that track citizens browsing, purchasing and other activities on the internet.

11. This overview analysis is focused on Government-led surveillance and the gaps in protection which currently exist in the international legal framework.

12. The surveillance and/or monitoring and/or profiling of citizens by corporations will be the subject of a separate report.

What do we understand by a comprehensive legal framework?

13. A comprehensive legal framework protecting citizens' privacy in cyberspace is one which provides both safeguards and remedies for all facets of the citizens' presence in cyberspace, irrespective of the fact if the threat to privacy comes from inside that citizen's country or from outside it.

14. Tension has continued to build up in cyberspace, with the privacy of many responsible citizens being put at risk by the behaviour of State actors in the form of cyber-surveillance, cyber-espionage and elements of cyber-war.

Problem Statement

15. In cyberspace, the citizen may be surveyed in both a domestic situation by his or her own Government, or else in a transboundary/transnational situation by a Government which is not his/her own. The case studies referenced below outline a fraction of some of the ways in which a citizen in one country finds him/herself subject to infringement of their privacy by their own Government or another State actor.

16. Where a citizen is subject to surveillance by his/her own Government then the safeguards and remedies must normally be sought within domestic law. Where a citizen is subject to surveillance by a State which is not his own, obligations of both the State conducting the surveillance and the State where that person is physically located are relevant; yet a remedy becomes harder to seek, because in practice most states accord the citizens of other States a lower level of protection than that accorded to their own citizens, in breach of the prohibition of discrimination found in articles 4, and 26 of the ICCPR.

17. For individuals not to suffer interferences in their right to privacy, they firstly need to benefit from safeguards which exist within domestic law, in other words, their Government should be subject to a whole set of regulatory procedures provided for by the law of that State, and which would include precautionary measures designed to ensure that surveillance cannot be initiated until or unless, it is proven to an independent and competent authority that this surveillance is legal, necessary and proportionate to objective pursued, "solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society" (UDHR, Art. 29(2).

Summary overview of protection gaps

18. In summary: the United Nations has 193 sovereign Member States and two non-member observer States, all of them capable of having their own independent systems/structures such as domestic legislation and data protection authorities.

19. More than 33 percent of United Nations Member States, i.e. over 70 countries, have no privacy law at all.

20. Out of the remaining 125 United Nations Member States which do have one form of privacy law or another, (for an outline of these states please see article by Professor Graham Greenleaf in Appendix Two attached) less than 65 have certain key fundamental characteristics such as a truly independent data protection authority or truly strict enforceable safeguards and remedies. Thus, these laws are not homogeneous and the level of protection of privacy differs quite widely from one country to the next.

21. The types of laws mentioned in Graham Greenleaf's article are mostly those intended to cover the use of personal data by companies or state departments outside the law enforcement and national security sector. Most of them are therefore not intended to adequately and comprehensively cover the use of surveillance by intelligence agencies.

22. More than 80 percent of the United Nations Member States do not have any law which protects privacy by adequately and comprehensively overseeing and regulating the use of domestic surveillance.

23. 100 percent of existing State legislations concerning the oversight of domestic intelligence within United Nations Member States require amendment and reinforcement.

24. 75 percent of United Nations Member States have no system of detailed safeguards or remedies to which they can readily turn to for cases of surveillance upon their citizens by other states. Even where remedies for citizens exist within the courts of those States, these courts often lack jurisdiction over the surveillance behaviour of other State actors.

25. 25 percent of United Nations Member States — those within the European region encompassed by the Council of Europe, have agreed to a basic principle in the application of privacy law to state security: by agreeing to Article 9 of Convention 108 they have accepted that measures can only limit the right to privacy where these measures are provided for by law and are necessary and proportionate in a democratic society.

26. This however means that it is only the very highest principles that have been agreed to, even in European states with more developed legislation on the right to privacy and this is mostly applied in the case of domestic intelligence. The situation relating to foreign intelligence is much more fluid, elastic. What actually constitutes a necessary and proportionate measure in a democratic society then needs to be translated into very detailed legislation and this is still very much work-in-progress all across Europe. Belgium, the Netherlands and the United Kingdom are some of the European states currently reviewing

their legislation in order to improve compliance with basic principles in a detailed manner. France has done so in 2015 but intends to re-visit its legislative framework in the near future.

27. Even where legislation exists regarding the oversight of intelligence it is often largely silent on what happens when personal data is shared across borders and what further safeguards should be put in place in such cases.

28. In the absence of more detailed regulation, several United Nations Member States have to rely on their existing legislative and judicial frameworks, often at the national constitutional or the regional level in order to develop remedies and safeguards on the hoof. This works slowly but relatively well at the European levels where the European Court of Justice and the European Court of Human Rights often have pan European reach with their judgments about surveillance and privacy.[2] This however is not a completely satisfactory solution since it is one ex post. Very preferably citizens wish to have their privacy protection provided ex ante and this, especially to protect themselves against or minimize intrusion. In order to resolve problems of jurisdiction in cyberspace, this can be only provided by detailed international law which does not yet exist in the surveillance sector, including in the European region. If the remedies are unclear and imperfect in Europe where the European Court of Human Rights has relatively worked well with over 100,000 cases decided since it was established in 1959, the situation outside Europe is even more concerning. In the Americas, the Inter-American Court of Justice established in 1979 has cross-country reach, as so has in in Africa the recently set-up (2006) African Court for Human and People's Rights. Both courts strive but struggle. The United States signed but never ratified the American Convention on Human Rights and, unlike the European human rights system, individual citizens of Member States of the Organization of American States cannot take their cases directly to the Inter-American Court, having to refer first to the Inter-American Commission on Human Rights. Likewise, only seven African states have signed the protocol empowering their regional court to receive petitions from non-governmental organizations and individuals. These limitations substantially weaken the reach of these regional courts. Moreover, in Asia or the Pacific there is no regional court to turn for infringements of privacy whether caused by domestic intelligence or foreign intelligence.

29. The United Nations Human Rights Committee plays a very important role in the protection of human rights, but once again is largely an ex post forum and cannot be expected to provide in-depth regulation and governance structures, which are the required minimum adequate legal response to questions like transborder data flows and cross-border espionage and surveillance.

[2] *The Snowden revelations – 6 June 2013 –ongoing reverberations across Europe*

The revelations over mass surveillance and other privacy –intrusive programmes carried out by the signals intelligence arms of the United Kingdom and United States intelligence communities have not really receded. They have been followed by legislative changes in both countries, sometimes imposing more constraints and safeguards, on other occasions legitimizing existing practices. The unilateral nature of transborder forays by United States and/or United Kingdom agencies into Belgium, Brazil, France, Germany and other countries led to a great deal of concern which still finds its reverberations in various fora, international and otherwise. Both countries are still struggling to find the right formula to frame their behaviour in cyberspace such that, for example, the legislative measures of the United Kingdom would be found necessary and proportionate by either the European Court of Human Rights or the European Court of Justice. The United Kingdom's intelligence services were found to be in default on several counts by the UK's own Investigatory Powers Tribunal while the United Kingdom law on bulk collection of metadata has been declared disproportionate by the European Court of Justice on the 21st December 2016. An important decision in this respect is also being expected in a case first heard by the European Court of Human Rights on 7th November 2017, Big Brother Watch and Others v. the United Kingdom (no. 58170/13), Bureau of Investigative Journalism and Alice Ross v. the United Kingdom (no. 62322/14) and 10 Human Rights Organisations and Others v. the United Kingdom (no. 24960/15).

30. In order to better understand the protection needs in the privacy area, one has to take the Yahoo cases[3] cited below and ask "which ex ante safeguards should have been applied by which country in order to protect citizens in, say France, from having their Yahoo e-mail account privacy infringed and what ex post remedies are available to that same French citizen?" The answers to these questions can only be provided by a detailed international law regime which has yet to be worked out. The Human Rights Committee's interpretative advice of ICCPR's article 17 should be a last resort; it cannot be the primary mechanism designed to protect the privacy of billions of people who use the Internet on a daily basis.

[3] The following two cases are being cited for purposes of illustrating a problem area but are not here being represented as facts proving certain types of behaviour by the United States or Russian authorities. The Special Rapporteur on the right to privacy reserves the right to investigate these cases separately through Letters of Allegation and until doing so remains neutral on the accuracy or otherwise of media and governmental reports on the subject:

Case 1: Privacy of 500 million Yahoo! users infringed – 15 March 2017

Formal indictments were brought in the United States of America by the Justice Department, which announced on 15 March 2017 that the "indictments of two Russian spies and two criminal hackers in connection with the heist of 500 million Yahoo user accounts in 2014, marking the first United States criminal cyber charges ever against Russian government officials. The indictments target two members of the Russian intelligence agency FSB, and two hackers hired by the Russians. The charges include hacking, wire fraud, trade secret theft and economic espionage, according to officials."

While this case remains sub judice and therefore the evidence available has not yet had time to be exhaustively evaluated by the court in question, the nationality of the accused and the locus of the judicial proceedings are almost immaterial for the purposes of this observation. The point here is that the spread of the damage was global, possibly the largest or one of the largest intrusions in history on the private e-mail accounts of five hundred million Yahoo! users spread across the planet. If it transpires that the men indicted were not responsible after all, we are still left with the problem of the nature and scale of the attack in addition to the instability induced by public accusations made against Russia. If the guilt of the accused is eventually proved beyond reasonable doubt then the problem would be compounded by the involvement of state officials who may or may not have been acting on instructions. Either way the suspicion of their acting as agents of the Russian state is already a destabilising factor in international relations and threatening all forms of peace, above and beyond cyber-peace. The violation of the personal space of hundreds of millions of internet users has not, to date, attracted much attention but it remains a source of major concern to those involved, over and above the charges actually made in the indictment.

Case 2: Privacy of 500 million (?) Yahoo! users breached by United States agency (reported 4th October 2016)

If you're a Yahoo! e-mail user, if it's not one government hacking into your e-mail account or scanning your incoming e-mail, then it's another. Or at least un-contradicted media reports so suggest. For some time during the period 2014–2016, hundreds of millions of Yahoo! e-mail users apparently not only suffered the most massive hack in history as already mentioned above (allegedly by a combination of Russian criminal and state-connected persons) but also had their incoming mail scan-read on the orders of a United States Government agency. There are multiple causes for concern here. Firstly, all those Yahoo! users within the United States may arguably claim that such searches violated their Fourth Amendment rights under the United States constitution, although the scan-reading was carried out in terms of lower-level United States law (FISA). Secondly, it should be clear to all concerned that well more than half of those five hundred million Yahoo users are not United States citizens and would need to seek recourse elsewhere for protection of their fundamental and universal right to privacy…but where to do so is the obvious question. Even if this were ever to be considered a proportional measure – and that is a contentious point in its own right, unless there were to be an international agreement that this would constitute appropriate state behaviour in cyberspace, hundreds of millions of citizens world-wide yet again find themselves without any effective safeguards or remedies when it comes to their fundamental right to privacy.

31. Thus it should be glaringly evident from the above summary that huge gaps exist in the legal protection of privacy at both the national and international levels. Unless and until it will be possible for any citizen, anywhere, irrespective of passport held, to enjoy privacy protection without borders and privacy remedies across borders, then it cannot be said that "a clear and comprehensive legal framework exists". In order to create such a clear and comprehensive legal framework it is essential that an international legal regime regulating issues of jurisdiction in cyberspace be properly developed, with a commonly agreed set of principles to establish what state behaviour in cyberspace and that especially related to surveillance and cyber-espionage, is acceptable, why and when.