



Asamblea General

Distr. general
30 de agosto de 2016
Español
Original: inglés

Septuagésimo primer período de sesiones

Tema 69 b) del programa provisional*

**Promoción y protección de los derechos humanos:
cuestiones de derechos humanos, incluidos otros medios
de mejorar el goce efectivo de los derechos humanos y
las libertades fundamentales**

El derecho a la privacidad**

Nota del Secretario General

El Secretario General tiene el honor de transmitir a la Asamblea General el informe del Relator Especial sobre el derecho a la privacidad, Sr. Joseph A. Cannataci, de conformidad con lo dispuesto en la resolución [68/167](#) de la Asamblea General y la resolución [28/16](#) del Consejo de Derechos Humanos.

* [A/71/150](#).

** Este informe se ha presentado fuera de plazo para incluir información recibida recientemente.



Informe del Relator Especial sobre el derecho a la privacidad

Resumen

El presente informe es el primero que presenta el Relator Especial sobre el derecho a la privacidad a la Asamblea General. Se redactó poco más de un año después de que el Relator Especial asumiera el cargo el 1 de agosto de 2015, y exactamente cinco meses después de que el Relator Especial presentara su primer informe al Consejo de Derechos Humanos el 9 de marzo de 2016. Hasta entonces, el Relator Especial se había centrado en poner de relieve una serie de temas que, según se había desprendido de sus numerosas consultas con múltiples partes interesadas, constituían esferas de trabajo fundamentales para la protección de la privacidad en la era digital.

En el período intermedio de cinco meses, el Relator Especial definió su primer conjunto de cinco prioridades, que se describen en el presente informe y en las que ha comenzado a trabajar en paralelo. Esas prioridades se denominan “líneas de acción temáticas” sobre macrodatos y datos abiertos; seguridad y vigilancia; datos sanitarios; datos personales procesados por las empresas; y “una mejor comprensión de la privacidad”. La metodología elegida por el Relator Especial prevé el establecimiento de un equipo de tareas —algunos lo llamarían grupo de trabajo— compuesto por voluntarios muy experimentados y no remunerados. Se está creando un grupo de trabajo para cada una de las cinco líneas de acción temáticas, y se espera que cada uno de ellos trate de ayudar al Relator Especial en la investigación pertinente y la redacción de un estudio temático que posteriormente sería objeto de un informe al Consejo de Derechos Humanos o la Asamblea General, que se presentaría durante el período 2017-2018.

El Relator Especial es partidario de maximizar la distribución geográfica, la diversidad cultural y étnica, la representación de los interesados y el equilibrio de género en cada uno de estos equipos de tareas o grupos de trabajo. Así, por ejemplo, el Equipo de Tareas sobre Macrodatos y Datos Abiertos estará presidido por David Watts, Comisionado para la Privacidad y la Protección de Datos del estado de Victoria, en Australia, mientras que el Equipo de Tareas sobre Datos Sanitarios estará presidido por Steve Steffensen, Jefe del Sistema de Aprendizaje en Salud de la Facultad de Medicina de Dell en Austin (Texas, Estados Unidos de América). En el momento de redactar el presente informe, el Relator Especial seguía llevando a cabo el proceso de contratación de los presidentes y miembros de algunos de los equipos de tareas. La composición exacta de cada equipo de tareas se anunciará en el momento oportuno, probablemente en marzo de 2017. Se prevé que cada equipo de tareas convoque reuniones y organice eventos públicos, semipúblicos y a puerta cerrada, según proceda, a fin de reunir elementos de información y definir opciones sobre estrategias posibles que ofrecerían mejores salvaguardias y medios de defensa para la privacidad en un determinado sector de actividad.

Así pues, el primer evento organizado por el Equipo de Tareas sobre Seguridad y Vigilancia fue la creación del Foro Internacional de Supervisión de los Servicios de Inteligencia (IIOF2016), en cuya reunión que se celebrará en Bucarest en octubre de 2016 se prevé la participación de varias docenas de organismos de supervisión y comités parlamentarios. Esto permitirá identificar colectivamente los problemas que plantea la labor de reunión de datos para la privacidad y la libertad de expresión, así como las mejores prácticas que podrían ofrecer mejores salvaguardias y medios de defensa en dicha labor. Entretanto, el Equipo de Tareas sobre “Una Mejor Comprensión de la Privacidad” ya ha organizado su primer evento en Nueva York, los días 19 y 20 de julio de 2016. Está previsto que, de los cinco Equipos de Tareas, este sea el último en informar, y sin duda no antes de 2018, dado que probablemente sea necesario celebrar varias otras consultas en diversas regiones, entre ellas África, América del Sur, Asia, Australia y Europa. El Equipo de Tareas ya ha comenzado a reunir elementos de información sobre conceptos como la relación entre la privacidad y el derecho fundamental general al libre desarrollo de la personalidad. Se prevé que sus actividades constituyan un proceso continuo que oriente a los demás Equipos de Tareas creados por el Relator Especial y aproveche las conclusiones extraídas por estos.

Si bien los cinco Equipos de Tareas proporcionan el enfoque temático, el Relator Especial también ha seguido supervisando las tendencias en varias docenas de países y ha puesto en marcha un programa de visitas oficiales a los países que garantizan la máxima interacción posible con el mayor número posible de interesados durante cada visita. En los cinco meses transcurridos entre marzo y agosto de 2016, el Relator Especial participó en múltiples actividades, a veces durante un período de hasta una semana de duración, 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. En los próximos meses se prevé que el Relator Especial visite, con carácter tanto oficial como oficial, España, los Estados Unidos, Francia, Indonesia, Israel, Marruecos, Irlanda del Norte (Reino Unido de Gran Bretaña e Irlanda del Norte), África Subsahariana y América del Sur. Este intenso programa de trabajo se lleva a cabo con la asistencia directa de los Gobiernos, los comisionados para la protección de la privacidad y los datos, institutos de derechos humanos, organizaciones no gubernamentales y universidades.

Índice

	<i>Página</i>
I. Introducción.....	5
A. Punto de partida	5
B. Comentarios iniciales e iniciativas de seguimiento	5
II. Principales actividades llevadas a cabo por el Relator Especial	5
A. Asignación de recursos al mandato del Relator Especial.....	5
B. Planificación y puesta en marcha de múltiples actividades en relación con el mandato	8
C. Participación en diversos eventos	12
III. Novedades importantes y cuestiones sustantivas, marzo a julio de 2016	14
A. El derecho a guardar silencio <i>nemo tenetur se ipsum accusare</i> : ¿debería un teléfono inteligente ser un testigo al que se le pueda requerir atestiguar, o podría constituir una violación de la privacidad demasiado grave?	14
B. Conservación de datos, vigilancia masiva y aún más cifrado	20
C. Mayor reconocimiento de la relación entre privacidad y personalidad	25
IV. Conclusiones	25

I. Introducción

A. Punto de partida

1. Este informe se presentará a las Naciones Unidas para su traducción antes de la reunión de la Asamblea General de octubre de 2016, en torno al 9 de agosto de 2016, es decir, transcurridos unos 18 meses desde que el Consejo de Derechos Humanos estableciera por primera vez un mandato sobre el derecho a la privacidad en su resolución [28/16](#) y un año después de que el titular asumiera el nombramiento. En este momento, el Relator Especial confirma que las iniciativas adoptadas hasta la fecha han recibido una gran cantidad de comentarios, en su mayoría de carácter positivo. El presente informe describirá adónde han llevado los esfuerzos del Relator Especial hasta la fecha y en qué se centrarán principalmente las actividades en un futuro próximo.

B. Comentarios iniciales e iniciativas de seguimiento

2. En marzo de 2016, ya se presentó un plan de acción de diez puntos en el primer informe al Consejo de Derechos Humanos (véase [A/HRC/31/64](#), párr. 46). Los comentarios recibidos sobre el plan de acción de diez puntos fueron muy positivos. Por consiguiente, el Relator Especial seguirá ocupándose de estas cuestiones y procurará presentar los resultados tangibles alcanzados en cooperación con todas las partes interesadas durante el mandato.

3. La experiencia acumulada a lo largo de los primeros 12 meses de desempeño del mandato, así como en la supervisión de los acontecimientos recientes en la esfera de la privacidad, ha dejado claro que algunas cuestiones exigen respuestas aún más rápidas y decisivas que otras, y, de esta suerte, se ha definido el primer conjunto de cinco prioridades. El Relator Especial se propone adoptar medidas apropiadas y presentar los resultados de la investigación de estas esferas prioritarias en informes temáticos separados.

II. Principales actividades llevadas a cabo por el Relator Especial

A. Asignación de recursos al mandato del Relator Especial

4. Las batallas no pueden ganarse si no se tienen tropas para librarlas. Dado que el mandato es nuevo, el Relator Especial se vio ante una situación administrativa en la que no existía equipo, y ha tenido que dedicar un tiempo considerable a la búsqueda de recursos para su mandato fuera de las Naciones Unidas. Aun cuando la cantidad y la calidad de los recursos aportados por las Naciones Unidas hubieran sido perfectos —y no lo fueron—, la labor del Relator Especial no puede realizarse adecuadamente sin una cantidad considerable de recursos adicionales a los facilitados por las Naciones Unidas. Hacer un seguimiento de la legislación sobre privacidad y las actividades de vigilancia en más de 190 Estados es una tarea que requiere varias docenas de empleados. Reunirse con representantes de la sociedad

civil y comprender sus preocupaciones, así como interactuar continuamente con las empresas, los organismos encargados de hacer cumplir la ley, los servicios de inteligencia y los encargados de la formulación de políticas, también requieren una inversión considerable de tiempo y esfuerzo por parte del personal. Organizar eventos de consulta en las cinco líneas de acción temáticas que se reseñan a continuación exige igualmente un importante esfuerzo por parte del personal. Casi ninguno de estos esfuerzos del personal procede actualmente de fuentes de las Naciones Unidas, máxime teniendo en cuenta que el tipo de personal necesario debe poseer conocimientos técnicos en los ámbitos correspondientes y ser especialista en privacidad. Baste decir que, en la actualidad, alrededor del 90% de los fondos destinados al personal que presta asistencia a la labor del mandato y aproximadamente el 80% de los gastos relacionados con viajes derivados del mandato deben sufragarlos fuentes ajenas a las Naciones Unidas. Además, los importantes obstáculos administrativos dentro del sistema hacen difícil centrar la atención en la parte sustantiva del mandato.

5. En cuanto a los recursos, decir que el apoyo prestado por la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (ACNUDH) al mandato del Relator Especial dista mucho de ser satisfactorio es quedarse muy corto. De acuerdo con la máxima latina *contra factum no argumentum est*, dejemos que los hechos hablen por sí solos:

a) Lo que el Relator Especial necesita —y quiere— no son burócratas del Cuadro de Servicios Generales, sino personal con conocimientos especializados en privacidad: el tipo de conocimientos que solo se adquieren mediante capacitación formal, cualificaciones y la experiencia directa. El Relator Especial así lo señaló al personal directivo superior de procedimientos especiales del ACNUDH, y, de hecho, en febrero de 2016 se publicó una convocatoria de candidaturas para un puesto del Cuadro Orgánico (de categoría P-3) de Oficial de Derechos Humanos en la que se indicaba una preferencia por los candidatos con cualificaciones y experiencia en privacidad. Se ha notificado al Relator Especial que se recibieron 349 candidaturas en respuesta a esa convocatoria, pero que en ningún momento se tuvo jamás en cuenta el contenido de dichas candidaturas. El Relator Especial no ha podido ver ninguna de estas candidaturas, pero algunas organizaciones no gubernamentales le han informado de que conocen candidatos con un doctorado en Privacidad y varios años de experiencia en trabajos relacionados con la privacidad;

b) El personal directivo superior del ACNUDH responsable del mandato del Relator Especial siguió ignorando por completo las candidaturas recibidas en la convocatoria pública para la presentación de candidaturas, y el 4 de agosto de 2016 informó al Relator Especial de que se había nombrado a un Oficial permanente de Derechos Humanos de “una lista interna de candidatos” para ponerlo a su disposición. Este Oficial de Derechos Humanos no tiene capacitación formal o cualificaciones en privacidad ni sólidos conocimientos o experiencia en la materia, tan solo experiencia secundaria en cuestiones relativas a la privacidad. El 8 de agosto, el Relator Especial escribió oficialmente al Presidente del Consejo de Derechos Humanos solicitando su intervención, distanciándose por completo de este proceso de contratación y expresando sus profundas reservas con respecto a la equidad del proceso y sus resultados;

c) Hasta el momento de redactar el presente informe, en el plazo de 12 meses se ha asignado al Relator Especial un total de un Oficial de Derechos Humanos en todo momento, siendo el actual el tercero de una sucesión de personal temporario. Ha habido una ocasión en que, debido a complicaciones contractuales, el Oficial de Derechos Humanos no estuvo disponible durante todo un mes natural. Ninguno de los Oficiales de Derechos Humanos tenía capacitación formal o cualificaciones en privacidad o experiencia en la gestión de cuestiones de privacidad, aunque el último Oficial de Derechos Humanos asignado al mandato (en julio de 2016), y que podría resultar ser más permanente, ha adquirido alguna experiencia limitada en el tratamiento de cuestiones relativas a la privacidad desde la perspectiva del mandato sobre la libertad de expresión. Con independencia de lo personalmente agradables o lo entendidos en otras esferas de derechos humanos que puedan haber sido los Oficiales de Derechos Humanos asignados, en esas circunstancias resulta muy difícil lograr y mantener la continuidad y la eficiencia;

d) El 4 de agosto de 2016 se informó al Relator Especial de que, además del Oficial permanente de Derechos Humanos mencionado en el apartado b) anterior, que se pondría a disposición del Relator Especial a tiempo completo al 1 de septiembre de 2016, posiblemente se contrataría a dos personas para ocupar, a tiempo parcial, un puesto de categoría P-3 y un puesto del Cuadro de Servicios Generales (Auxiliar Administrativo), respectivamente, durante o después de septiembre. Dado el nivel de eficiencia demostrado hasta la fecha, no tenemos muchas esperanzas;

e) El nivel de ineficiencia es tal que siguen pendientes reembolsos parciales de gastos en concepto de viajes de las Naciones Unidas realizados en el cuarto trimestre de 2015 —y esto a un funcionario no remunerado como el Relator Especial—.

6. En el párrafo anterior se ha descrito con cierto detalle (pero en ningún caso de manera integral) la insuficiencia del apoyo ofrecido por el ACNUDH, a fin de que ni la Asamblea General ni el Consejo de Derechos Humanos alberguen ilusiones en cuanto a que el Relator Especial está realizando su labor gracias a un apoyo increíblemente eficiente o generoso del ACNUDH. No deseo volver sobre este asunto en futuros informes. Si la Asamblea o el Consejo no vuelven a oír al Relator Especial hablar de la cuestión, deberían suponer que la situación no ha mejorado en modo alguno que merezca observaciones específicas. Por otra parte, este no es un ejercicio de reparto de culpas: dejaré que un Secretario General entrante y, esperemos, con una mentalidad reformista decida si la situación descrita en los párrafos anteriores obedece a un sistema irremediablemente ineficiente que debe ser objeto de revisión con carácter urgente, o bien a un círculo de funcionarios públicos internacionales egoístas que tienen mucho más interés en proseguir sus cómodas gestiones en lugar de ofrecer a un Relator Especial el apoyo cualitativo y cuantitativo necesario para desempeñar debidamente el mandato. Si usted representa a un Estado o una organización que cree verdaderamente en el mandato y en su importancia y desea contribuir, sírvase comunicarse directamente con el Relator Especial a fin de estudiar distintas opciones sobre la forma en que podría prestarse más apoyo.

B. Planificación y puesta en marcha de múltiples actividades en relación con el mandato

7. Pese a los problemas administrativos y de recursos que acaban de exponerse, el Relator Especial y sus equipos, con el apoyo de numerosos agentes de la sociedad civil y otros interesados comprometidos con la causa, pudieron poner en marcha múltiples actividades. Estas pueden clasificarse de manera general como la supervisión continua de las actividades en los distintos Estados y líneas de acción temáticas, como se explica al detalle a continuación.

8. El desarrollo de nuevas actividades de vigilancia, leyes que permiten la vigilancia y leyes de privacidad en varias docenas de Estados Miembros de las Naciones Unidas sigue siendo parte de la actividad esencial de supervisión permanente que el Relator Especial realiza a diario. Esta labor exige examinar cada nueva tecnología desplegada y cada nueva ley propuesta e investigar una serie de denuncias presentadas a la atención del titular del mandato especial por las personas afectadas o por la sociedad civil. Esta actividad de supervisión es una parte esencial del proceso de recopilación de elementos de información que orienta al Relator Especial a la hora de elegir qué países visitará de manera oficial y oficiosa.

9. Además de las actividades específicas para cada país, que exigen en sí mismas largo tiempo, se ha dedicado mucha atención y esfuerzo a las prioridades temáticas. Algunas esferas del plan de acción de diez puntos expuesto al Consejo de Derechos Humanos en el informe presentado en marzo de 2016 requieren una atención inmediata y una acción simultánea. Estas esferas se han establecido cuidadosamente y ahora se tratarán en forma de líneas de acción temáticas¹. En esta primera fase de actividad se han creado cinco líneas de acción temáticas, una para cada una de las siguientes prioridades: a) macrodatos y datos abiertos; seguridad y vigilancia; datos sanitarios; datos personales procesados por las empresas; y “una mejor comprensión de la privacidad”. Se prevé que cada una de estas líneas de acción desarrolle su propia dinámica, a la vez que interactúe con otras líneas de acción temáticas, y permita al Relator Especial preparar un informe temático en el momento en que la investigación y el debate dentro de una línea de acción específica estén a punto.

¹ Puede obtenerse más información sobre el tema en el artículo del blog de Joseph Cannataci titulado “Parallel streams of action (TAS) for the mandate of the United Nations Special Rapporteur for privacy and the first set of priorities” (Líneas de acción paralelas para el mandato del Relator Especial de las Naciones Unidas sobre el derecho a la privacidad y primer conjunto de prioridades), publicado el 3 de junio de 2016. Disponible en <https://www.privacyandpersonality.org/2016/06/privacy-and-personality-blog-3-parallel-streams-of-action-tas-for-the-mandate-of-the-un-special-rapporteur-for-privacy-and-the-first-set-of-priorities/>.



10. La metodología elegida por el Relator Especial prevé el establecimiento de un equipo de tareas —algunos lo llamarían grupo de trabajo— compuesto por voluntarios muy experimentados y no remunerados. Habría un grupo de trabajo para cada una de las cinco líneas de acción temáticas, y se espera que cada uno de ellos trate de ayudar al Relator Especial en la investigación pertinente y la redacción de un estudio temático que posteriormente sería objeto de un informe al Consejo de Derechos Humanos o la Asamblea General, que se presentaría durante el período 2017-2018.

11. La priorización de los macrodatos y datos abiertos se vio confirmada por investigaciones secundarias y especialmente en diversas reuniones de partes interesadas y actividades de investigación celebradas durante las visitas a Alemania, Australia, Austria, Dinamarca, los Estados Unidos de América, Francia, Italia, Letonia, Nueva Zelanda, los Países Bajos y Suiza en el período comprendido entre marzo y julio de 2016. Por tanto, en mayo de 2016 se creó un Equipo de Tareas sobre Macrodatos y Datos Abiertos, que David Watts, Comisionado para la Protección de la Privacidad y los Datos del estado de Victoria, en Australia, aceptó presidir por invitación del Relator Especial. En junio se comenzó a trabajar en la elaboración de un bosquejo de los objetivos de trabajo de dicho grupo y la contratación de los primeros miembros. El 20 de julio de 2016, el Sr. Watts y el Relator Especial presentaron el primer esbozo del trabajo propuesto en un evento coorganizado por el Relator Especial en Nueva York, e invitaron a que se formularan observaciones y a que los voluntarios trabajaran en dicho grupo. Desde entonces se han recibido ofertas de expertos voluntarios procedentes del Brasil, el Canadá, los Estados Unidos, Francia y el Senegal. Se espera que la composición del Equipo de Tareas y el primer esbozo de los objetivos y el mandato se publiquen antes del final de octubre de 2016. Este Equipo de Tareas también solicita el apoyo de organizaciones independientes que deseen contribuir a soluciones técnicas de ensayo de capacidad que pretendan anonimizar con éxito los datos personales de forma que no sea posible volver a identificarlos en el contexto de análisis de macrodatos capaces de hacer una triangulación con fuentes de datos abiertos.

12. Nunca cupo la menor duda de que la seguridad y la vigilancia ocuparían un lugar destacado en la lista de prioridades del Relator Especial. La complejidad de la esfera, por cuanto aúna los intereses tanto de los organismos encargados de hacer cumplir la ley como de los servicios de seguridad e inteligencia, y está interrelacionada con las actividades de algunas grandes empresas, ha hecho necesario empezar por dividir los temas que deberán abordarse en subconjuntos más pequeños, haciéndose en todos ellos especial hincapié en señalar y reforzar las salvaguardias y los medios de defensa de la privacidad. La primera gran iniciativa adoptada por el Relator Especial en este sector fue crear el Foro Internacional de Supervisión de los Servicios de Inteligencia (IIOF2016), en cuya reunión que se celebrará en Bucarest en octubre de 2016 se prevé la participación de varias docenas de organismos de supervisión y comités parlamentarios. Esto debería permitir identificar colectivamente los problemas que plantea la labor de reunión de datos para la privacidad y la libertad de expresión, así como las mejores prácticas que podrían ayudar al Relator Especial y todos los interesados a encontrar mejores salvaguardias y medios de defensa. El Relator Especial llevó a cabo gran parte de la labor preparatoria para organizar el IIOF2016 entre marzo y julio de 2016, y la respuesta de los principales Estados Miembros de las Naciones Unidas ha sido muy alentadora, pues algunos Estados ya han confirmado su participación en esta reunión, que, de tener éxito, podría mantenerse como un evento periódico que contribuya con aportaciones a los informes, las recomendaciones y otras iniciativas del Relator Especial. El Relator Especial aprovecha esta oportunidad para agradecer públicamente a los numerosos Estados Miembros de las Naciones Unidas que han participado en este ejercicio, especialmente los cuatro Comités de Supervisión de los Servicios de Inteligencia del Senado y el Parlamento de Rumania, que han aceptado su invitación a organizar conjuntamente el evento. Merece también reconocimiento la Agencia de los Derechos Fundamentales de la Unión Europea, que está apoyando este evento de diversas formas. Asimismo, se están llevando a cabo otros trabajos sobre la vigilancia en el marco del Equipo de Tareas sobre los Datos Personales Procesados por las Empresas (véase más abajo). Puede que más adelante se den a conocer públicamente otras iniciativas y trabajos en el sector.

13. La constante interacción del Relator Especial con las partes interesadas y sus investigaciones exhaustivas han confirmado que la creación, el procesamiento, la venta y la reventa de grandes cantidades de datos sanitarios sensibles siguen creciendo en todo el mundo. Estas prácticas no solo están institucionalizadas como parte del modelo empresarial en un pequeño número de países creadores de tendencias, sino que también se están intensificando por la tendencia en espiral ascendente de los consumidores a utilizar tecnologías ponibles, aplicaciones para teléfonos inteligentes y otras tecnologías portátiles que recogen y transmiten constantemente muchas formas de datos relativos a la salud y el estilo de vida potencialmente sensibles. Además, los experimentos en algunos países con la utilización de historiales médicos existentes para mejorar la capacidad de diagnóstico gracias a técnicas de inteligencia artificial también pueden convertirse en un motivo de creciente preocupación. Por otra parte, es evidente que el uso de datos sanitarios puede redundar en una serie de beneficios, como adelantos en la investigación médica. Algunos estudios de mercado independientes también sugieren que los pacientes están cada vez más preocupados por el hecho de que sus datos personales puedan utilizarse indebidamente. A fin de progresar en sus

esfuerzos en el sector de los datos sanitarios de forma estructurada, y tras un período de consultas con las principales organizaciones no gubernamentales en esta esfera, el Relator Especial se complace en anunciar que el Dr. Steve Steffenson, del Dell Hospital de la Universidad de Texas en los Estados Unidos, ha aceptado presidir el Grupo de Trabajo denominado MedITAS. Actualmente se está tramitando la contratación de los demás miembros del Grupo de Trabajo, y se prevé que el mandato preliminar que se ha elaborado se desarrolle más y se apruebe una vez que el Equipo de Tareas entre en funcionamiento a comienzos del cuarto trimestre de 2016.

14. El Relator Especial está aprovechando los contactos que mantiene con las principales empresas gracias a proyectos anteriores y en curso y, especialmente, su colaboración en el proyecto MAPPING (Managing Alternatives for Privacy, Property and Internet Governance), que cuenta con el apoyo de la Unión Europea, a fin de seguir examinando el impacto de la creciente utilización de datos personales por el sector empresarial en la privacidad. El Relator Especial sigue beneficiándose de los trabajos en curso con empresas en al menos tres componentes del proyecto MAPPING relacionados con el potencial del derecho internacional, los modelos empresariales y la privacidad, los cuales se espera ofrezcan nuevas aportaciones a la labor del titular del mandato especial en este sector, y también configuren (en el proyecto MAPPING) un documento de políticas y una hoja de ruta para que la Unión Europea los examine. Parte de esta labor también es pertinente para las actividades de vigilancia de los Gobiernos, y se espera que impulse una consulta conjunta en la materia con la sociedad civil en un evento organizado conjuntamente por el titular del mandato de Relator Especial y el proyecto MAPPING que se celebraría los días 15 y 16 de febrero de 2017. Cabe agradecer a una serie de empresas destacadas, como Microsoft, Google, Facebook, Apple y Yahoo!, así como a Global Network Initiative, que han seguido colaborando con el mandato del Relator Especial y con el proyecto MAPPING de una manera muy positiva. Todos los demás interesados pueden unirse a este proceso en el momento oportuno, y el Relator Especial invita a presentar manifestaciones de interés en esta cuestión, al igual que en las demás iniciativas de los Equipos de Tareas.

15. Una de las iniciativas a más largo plazo adoptadas por el Relator Especial es el Equipo de Tareas centrado en “Una Mejor Comprensión de la Privacidad”. La intención es que, de los cinco Equipos de Tareas, este sea el último en informar, y sin duda no antes de 2018, dado que probablemente sea necesario celebrar varias otras consultas en diversas regiones, entre ellas África, América del Sur, Asia, Australia y Europa. Este Equipo de Tareas ya ha comenzado a reunir elementos de información sobre conceptos como la relación entre la privacidad y el derecho fundamental general al libre desarrollo de la personalidad. Se prevé que sus actividades constituyan un proceso continuo que oriente a los demás Equipos de Tareas creados por el Relator Especial y aproveche las conclusiones extraídas por estos. También es uno de los equipos de tareas que dedica considerable atención a la relación entre el derecho a la privacidad y otros derechos fundamentales como la libertad de expresión y la libertad de (acceso a la) información. Las conversaciones preliminares entabladas con Human Rights Watch ya en septiembre de 2015 contribuyeron a impulsar la organización del primer evento de este Equipo de Tareas, titulado “Privacidad, personalidad y flujos de información”, celebrado en Nueva York los días 19 y 20 de julio de 2016. Este evento de dos días completó el

aforo de 90 personas en una sala de conferencias y se celebró gracias a la generosidad y los esfuerzos combinados de Human Rights Watch; el Brennan Center for Justice at New York University School of Law; Global Freedom of Expression at Columbia University; el proyecto MAPPING; el Departamento de Gobernanza y Política de Información de la Universidad de Malta; y el Grupo de Investigación STeP, dedicado a la seguridad, la tecnología y la privacidad en Internet, en la Universidad de Groningen, en los Países Bajos. Gracias también al Gobierno de Alemania por haber proporcionado al titular del mandato especial algunos de los fondos que apoyaron la participación mundial en este evento.

16. Si bien la perspectiva local (de los Estados Unidos) fue la que tuvo indudablemente mayor representación, también estuvieron presentes para compartir sus opiniones y percepciones participantes de Australia, el Brasil, el Canadá, Colombia, la India, la República de Corea, la región del Oriente Medio y Norte de África, Europa² y la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura. El objetivo principal de la reunión durante el primer día era trabajar para tener una comprensión más amplia y mejor de lo que significa la privacidad como derecho humano universal en la era digital y si este derecho debe entenderse más firmemente en el contexto de propiciar el desarrollo personal. El segundo día se centró en facilitar la comprensión y la elaboración de estrategias de promoción a fin de permitir el fomento más eficaz y firme del derecho a la privacidad en todo el mundo. Este acto sirvió como evento piloto de una nueva serie de eventos que abordarán la misma cuestión y se organizarán en todos los continentes para consolidar el mayor número posible de opiniones sobre el tema, a fin de procurar establecer y profundizar una comprensión más amplia de la privacidad y su interpretación en la era digital en beneficio de la comunidad mundial. Por lo tanto, aunque ya ha comenzado la planificación para el próximo evento, que se celebrará en Asia, el Relator Especial desea por la presente invitar a las partes interesadas en apoyar, organizar y participar en dichos actos en un futuro próximo a ponerse en contacto con él directamente.

17. En gran medida (aunque no exclusivamente) como parte de la labor emprendida para apoyar el mandato, el Relator Especial y su equipo también han creado un blog sobre la privacidad y la personalidad. Puede consultarse en www.privacyandpersonality.org.

C. Participación en diversos eventos

18. Además de las actividades expuestas más arriba, y también con el fin de alcanzar el objetivo de sensibilización sobre la privacidad descrito en el plan de acción de diez puntos, el Relator Especial ha participado en una serie de actividades desde el 3 de marzo de 2016, en particular:

² Concretamente, se examinó y debatió la concepción alemana de la “libre determinación de la información” y la protección de la privacidad (*Datenschutz*) como posible modelo para reforzar la comprensión de la privacidad como un derecho habilitante para desarrollar la personalidad. El Relator Especial agradece la contribución de Christian Hawellek, del Institut für Rechtsinformatik en la Leibniz Universität Hannover.

- a) El discurso inaugural pronunciado en el Instituto de Derecho Internacional de la Paz y los Conflictos Armados, en Bochum (Alemania), el 15 de marzo;
- b) La reunión con la Presidenta de la Comisión Nacional francesa sobre Informática y Libertades y el Grupo de Trabajo del Artículo 29 de la Unión Europea, celebrada en París el 18 de marzo;
- c) El panel en la Cumbre Mundial sobre Privacidad de la Asociación Internacional de Profesionales de la Privacidad, celebrada en Washington, D.C., el 5 de abril;
- d) El discurso de apertura pronunciado en el Simposio anual del *Wisconsin International Law Journal*, celebrado en Wisconsin el 8 de abril;
- e) El precongreso inaugural del Congreso anual de la Asociación de Responsables de la Protección de Datos (taller centrado en el Reglamento general de protección de datos y la función del responsable de la protección de datos de la Unión Europea), celebrado en Milán (Italia) el 18 de abril;
- f) El Foro Mundial sobre Futuros Digitales, Universidad de Columbia, celebrado en Nueva York el 25 de abril;
- g) Múltiples discursos de apertura y reuniones de interesados celebradas en la Semana de la Privacidad, en Wellington y Auckland (Nueva Zelanda), del 9 al 13 de mayo;
- h) Múltiples discursos de apertura y reuniones de interesados celebradas en la Semana de Sensibilización sobre la Privacidad, en Sydney y Canberra (Australia), del 14 al 18 de mayo;
- i) El acto sobre investigación e innovación en materia de seguridad de 2016, celebrado en La Haya los días 1 y 2 de junio;
- j) El panel “Privacidad en el próximo Gobierno” en la Conferencia sobre Protección de Datos 2016 del Electronic Privacy Information Center (EPIC), celebrada en Washington, D.C. el 6 de junio;
- k) El discurso de apertura en la Sexta Cumbre Internacional sobre el Futuro de la Privacidad de la Salud, celebrada en Washington, D.C. el 7 de junio;
- l) El evento de MAPPING y el Relator Especial con la participación de partes interesadas, organizado por Álvaro Bedoya en el Centro de Derecho de Georgetown sobre la Privacidad, celebrado en Washington, D.C. el 8 de junio;
- m) Reuniones con Google, Facebook y el Departamento de Estado de los Estados Unidos, celebradas en Washington, D.C. los días 9 y 10 de junio;
- n) La conferencia abierta y el discurso de apertura, actos celebrados en DataEthics.EU y el Instituto Danés de Derechos Humanos, en Copenhague, el 13 de junio;
- o) La mesa redonda de la Asociación para el Progreso de las Comunicaciones, celebrada en Ginebra el 14 de junio;

- p) La intervención en el taller organizado por el Comité Internacional de la Cruz Roja, celebrado en Ginebra el 14 de junio;
- q) El debate en línea con los miembros de Internet Society, celebrado en Ginebra el 14 de junio;
- r) La conferencia titulada “Convenio 108: de una realidad europea a un tratado mundial” del Consejo de Europa, celebrada en Estrasburgo (Francia) el 17 de junio;
- s) El Foro de los Derechos Fundamentales de la Agencia de los Derechos Fundamentales de la Unión Europea, celebrado en Viena los días 20 y 21 de junio;
- t) Las conversaciones de Alpbach: “Tiempo de compartir: lugares para todos”, en cooperación con el periódico *Wiener Zeitung*, celebradas en Viena el 22 de junio;
- u) El debate del Grupo de Trabajo 25 sobre “El papel y la responsabilidad de las empresas en el respeto de la privacidad en un contexto de mayor seguridad en Europa”, celebrado en Viena el 23 de junio;
- v) El Segundo Foro Europeo de Alfabetización Mediática e Informacional, celebrado en Riga del 27 al 29 de junio;
- w) La conferencia del Relator Especial sobre el derecho a la privacidad titulada “Privacidad, personalidad y flujos de información”, celebrada en Nueva York los días 19 y 20 de julio.

III. Novedades importantes y cuestiones sustantivas, marzo a julio de 2016

A. El derecho a guardar silencio *nemo tenetur se ipsum accusare*: ¿debería un teléfono inteligente ser un testigo al que se le pueda requerir atestiguar, o podría constituir una violación de la privacidad demasiado grave?

19. En el año 2016 se ha reabierto el debate sobre la importancia del cifrado de datos personales almacenados en dispositivos móviles o generados por estos. Cabe destacar, sin duda, los hechos relacionados con un teléfono inteligente utilizado por una persona que cometió un terrible atentado en San Bernardino (Estados Unidos) y los posteriores intentos de las autoridades de los Estados Unidos para tener acceso a los datos personales almacenados en el dispositivo fabricado por Apple Inc., que han captado la atención del público. El 2 de diciembre de 2015, un hombre y su mujer abrieron fuego contra una oficina gubernamental local en el sur de California. Como resultado de ello 14 personas murieron, y más de 20 personas resultaron gravemente heridas³. El Buró Federal de Investigaciones (FBI) de los Estados Unidos estaba interesado en la información que se había almacenado en el

³ Camila Domonoske, “San Bernardino shootings: what we know, one day after”, National Public Radio, 3 de diciembre de 2015. Disponible en www.npr.org/sections/thetwo-way/2015/12/03/458277103/san-bernardino-shootings-what-we-know-one-day-after.

dispositivo y sincronizado con el servicio de Apple de computación en la nube (iCloud). Aunque fue posible recuperar los datos almacenados externamente hasta el 19 de octubre de 2015 (cuando se interrumpió el almacenamiento de copias de seguridad), los datos que se almacenaron localmente en el teléfono inteligente no eran fácilmente accesibles para el FBI o Apple. El FBI intentó recurrir al marco jurídico para imponer a Apple la obligación de cambiar el software instalado en los teléfonos inteligentes a fin de hacerlos menos resistentes en caso de ataque de piratería. Cuando Apple se negó a acceder a la demanda, el FBI llevó el caso a los tribunales y ejerció presión sobre la empresa. Finalmente, el 28 de marzo de 2016, el FBI renunció a su batalla judicial contra Apple gracias a que pudo acceder a la información almacenada en el teléfono inteligente por otros medios⁴. “Desde el principio, nos opusimos a la petición del FBI de que Apple cree una puerta trasera en el iPhone porque creíamos que era un error y sentaría un peligroso precedente. Como resultado de la destitución del gobierno, nada de esto ha llegado a ocurrir”, afirmó Apple en una declaración tras el desistimiento de la instancia⁵. El Relator Especial, en el párrafo 30 de su informe de 9 de marzo de 2016, ha expuesto su posición de que permitir u ordenar puertas traseras al cifrado es una mala idea por muchas razones, que se resumen mejor en un documento de posición del Gobierno de los Países Bajos de 4 de enero de 2016. El caso de Apple no le ha hecho cambiar de opinión sobre ese aspecto del asunto. Los teléfonos inteligentes y otros dispositivos móviles plantean, sin embargo, otras cuestiones relacionadas con los derechos fundamentales que pueden afectar a la privacidad y que posiblemente deban decidirse antes de que pueda tener lugar o se pueda avanzar efectivamente en relación con la próxima fase de la “conversación” sobre cifrado. Uno de esos derechos es el derecho a guardar silencio.

20. Ahora que el caso de Apple contra el FBI ya no está *sub-judice* y, esperemos, las personas de todas partes pueden reflexionar con un poco más de claridad y menos apasionamiento, se señala respetuosamente que, teniendo en cuenta que se han vendido cientos de millones de teléfonos inteligentes de Apple en todo el mundo, se trata de una cuestión de interés mundial, y no de interés exclusivamente en los Estados Unidos. De igual manera, las mismas leyes que se aplicaron para juzgar y obligar a Apple a ayudar a los organismos encargados de hacer cumplir la ley a acceder a los datos en ese caso podrían utilizarse con otros fabricantes que han vendido muchos más cientos de millones de teléfonos inteligentes en todo el mundo que Apple, sobre todo porque cada vez más fabricantes están incorporando medios de protección criptográfica en sus productos. Parecería que las economías de escala implican que estamos avanzando hacia una situación en la que, primero, un tercio y,

⁴ Véanse los siguientes artículos publicados en *The Guardian*: Danny Yadron, Spencer Ackerman y Sam Thielman, “Inside the FBI’s encryption battle with Apple”, 18 de febrero de 2016. Disponible en <https://www.theguardian.com/technology/2016/feb/17/inside-the-fbis-encryption-battle-with-apple>; Danny Yadron, “San Bernardino iPhone: United States ends Apple case after accessing data without assistance”, 29 de marzo de 2016. Disponible en <https://www.theguardian.com/technology/2016/mar/28/apple-fbi-case-dropped-san-bernardino-iphone>; Danny Yadron, “FBI confirms it won’t tell Apple how it hacked San Bernardino shooter’s iPhone”, 28 de abril de 2016. Disponible en <https://www.theguardian.com/technology/2016/apr/27/fbi-apple-iphone-secret-hack-san-bernardino>.

⁵ Hilary Brueck, “This is Apple’s response to the FBI hacking into that iPhone”, 29 de marzo de 2016. Disponible en <http://fortune.com/2016/03/29/apple-response-fbi>.

a la larga, la mitad de la población mundial tendrá y usará un teléfono inteligente. Por lo tanto, como se verá más adelante, nos enfrentamos a un hecho simple: el teléfono inteligente es una tecnología omnipresente que tiene enormes consecuencias para la privacidad.

21. El Relator Especial expondrá aquí algunas observaciones preliminares en un intento de hacer avanzar el debate sobre los teléfonos inteligentes más allá de la privacidad, con la intención, en última instancia, de volver al debate de las preocupaciones fundamentales sobre la privacidad mejor informados por la confirmación o abnegación de los valores de la sociedad sobre “el panorama general”. El Relator Especial considera que deben examinarse otras normas de conducta apropiadas en la sociedad antes de que pueda darse una opinión más definitiva sobre algunos de los aspectos de la utilización de los teléfonos inteligentes que afectan a la privacidad.

22. Al igual que muchos otros derechos humanos fundamentales, la privacidad es un derecho dinámico, no un derecho estático. Durante miles de años ha habido una expectativa de privacidad y una preferencia por la privacidad, pero ello no quiere decir que el grado de protección del derecho a la privacidad o la comprensión de sus límites se haya mantenido invariable a medida que la tendencia se ha desplazado hacia una mayor protección. La privacidad se ha desarrollado a lo largo del tiempo, y se han identificado muchas pruebas antes de que se creara el mandato del Relator Especial y se nombrara al titular, lo que demuestra cómo ha variado la comprensión de la privacidad y el ejercicio del derecho en las dimensiones de tiempo, lugar y espacio⁶. A diferencia de lo que algunos puedan pensar, reconocer esta realidad no socava de manera alguna la existencia del derecho ni su universalidad. Por el contrario, hace que uno reflexione sobre el complejo conjunto de valores que sustentan el derecho y la forma en que debe cambiar nuestra comprensión del derecho conforme cambian las circunstancias, a fin de que sigan protegiéndose los valores subyacentes y, más aún, en la medida de lo posible, se asegure su mayor protección. El advenimiento y las aplicaciones de nuevas tecnologías, como el teléfono inteligente, son un ejemplo típico de hasta qué punto debemos actualizar nuestra comprensión de la privacidad. Como señaló el Sr. Samuel Alito, magistrado del Tribunal Supremo de los Estados Unidos, en la célebre causa de los Estados Unidos *Riley c. California* en 2014:

“No deberíamos aplicar mecánicamente la norma utilizada en la era predigital al registro de un teléfono móvil. Ahora, muchos teléfonos móviles en uso son capaces de almacenar y acceder a una cantidad de información, alguna muy personal, que nadie habría tenido nunca sobre su persona en versión impresa⁷.”

En este sentido, Alito coincide con la opinión mayoritaria expresada por el Presidente del Tribunal Supremo, John Roberts, de que:

⁶ Para tener una visión mucho más detallada de la valoración que hace el Relator Especial de la existencia y las dimensiones de tiempo, lugar y espacio de la privacidad a lo largo de toda la historia, véase Joseph A. Cannataci, ed., *The Individual and Privacy* (Farnham, Reino Unido, Ashgate Publishing, 2015).

⁷ Tribunal Supremo de los Estados Unidos de América, *Riley v. California*, decisión de 25 de junio de 2014, núm. 13-132. Disponible en https://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf.

“Los teléfonos móviles modernos no son simplemente otra utilidad tecnológica. Con todo lo que almacenan y todo lo que pueden revelar, contienen para muchos norteamericanos ‘las intimidades de la vida’. El hecho de que ahora la tecnología permite a una persona llevar esa información en la mano no hace que la información sea menos digna de la protección por la que lucharon los Fundadores⁷.”

Huelga decir que no son solo los norteamericanos quienes, consciente o inconscientemente, entregan “las intimidades de la vida” a sus teléfonos móviles. De hecho, cada persona de este planeta que tiene un teléfono inteligente ha confiado al dispositivo portátil que más utiliza las intimidades de su vida, independientemente de su credo, color, origen étnico, género, nacionalidad o ubicación geográfica. Esa es la razón por la que muchas de las observaciones formuladas en la causa *Riley c. California* son también de importancia mundial. El Relator Especial extraerá en esta sección amplias citas de esta causa de los Estados Unidos, por cuanto en ella se exponen algunos de los argumentos que deberían examinarse a continuación en el contexto general del litigio entre Apple y el FBI dondequiera que se planteen esas cuestiones en todo el mundo.

23. Como se explica en *Riley c. California*, los teléfonos móviles modernos son ahora una parte tan omnipresente e insistente de la vida cotidiana que el proverbial visitante de Marte podría llegar a la conclusión de que eran una característica importante de la anatomía humana⁷. Los magistrados del Tribunal Supremo señalaron con acierto que:

“Los teléfonos móviles difieren en un sentido tanto cuantitativo como cualitativo de otros objetos que una persona detenida podría tener consigo. El propio término ‘teléfono celular’ es engañoso; muchos de estos dispositivos son en realidad mini-ordenadores que también se pueden utilizar como un teléfono. Podrían fácilmente calificarse de cámaras, reproductores de video, agendas giratorias, calendarios, grabadoras, bibliotecas, diarios, álbumes, televisores, mapas o periódicos. Una de las características distintivas más notables de los teléfonos móviles modernos es su inmensa capacidad de almacenamiento. Antes de los teléfonos móviles, el registro de una persona se veía limitado por realidades físicas y, en general, tendía a constituir solo una pequeña intromisión en la intimidad⁷.”

Más de una vez, los magistrados del Tribunal Supremo de los Estados Unidos señalan que:

“Hay un elemento dominante que caracteriza los teléfonos inteligentes, pero no los archivos físicos. Antes de la era digital, la gente no solía llevar consigo un alijo de información personal sensible mientras realizaban sus tareas cotidianas. Ahora, la persona que no lleva consigo un teléfono móvil, con todo lo que contiene, es la excepción. Según un sondeo, casi tres cuartas partes de los usuarios de teléfonos inteligentes afirman encontrarse a una distancia no superior a 1,5 m de sus teléfonos la mayor parte del tiempo, y el 12% admite que incluso utiliza su teléfono en la ducha⁷.”

Los magistrados señalan igualmente la capacidad de los teléfonos inteligentes para ofrecer un perfil muy detallado y preciso de su usuario:

“Aunque los datos almacenados en un teléfono móvil se distinguen de los archivos físicos únicamente por la cantidad, algunos tipos de datos también son diferentes desde un punto de vista cualitativo. En un teléfono con posibilidad de conexión a Internet pueden encontrarse, por ejemplo, una búsqueda hecha en Internet y el historial del explorador, que podrían revelar los intereses privados o las inquietudes de una persona —acaso una búsqueda de determinados síntomas de una enfermedad, junto con visitas frecuentes a WebMD—. Los datos de un teléfono móvil también pueden revelar dónde ha estado una persona⁷.”

24. Lo más importante, quizá, es la percepción de los magistrados del Tribunal Supremo de los Estados Unidos de que el contenido de un teléfono móvil es tan grande en términos de cantidad y de carácter tan íntimamente privado que trasciende con creces el grado de privacidad amparado por la Cuarta Enmienda de la Constitución de los Estados Unidos, en el que el tradicional registro domiciliario supondría una intromisión:

“Por lo general, el registro de un teléfono móvil revelaría al Gobierno mucho más que el más exhaustivo registro domiciliario: un teléfono no solo contiene en formato digital muchos archivos sensibles previamente encontrados en el domicilio; también contiene una amplia gama de información privada que nunca se encuentra en un domicilio en ninguna forma, salvo el teléfono⁷.”

Así, los magistrados del Tribunal Supremo de los Estados Unidos demostraron cómo la nueva tecnología que encarnan los teléfonos inteligentes ha cambiado las reglas del juego y que en este momento (2014 —que alude a la dimensión de “tiempo”—), el “lugar” (los Estados Unidos —y el teléfono ubicado en los Estados Unidos—) donde se encontraban los datos personales había cambiado considerablemente a uno donde la portabilidad, la cantidad y la calidad de la información personal son capaces de alterar por completo e intensificar la dimensión de la privacidad del “espacio” personal.

25. Los magistrados del Tribunal Supremo de los Estados Unidos, en la causa *Riley c. California*, se ocuparon fundamentalmente de declarar ilegales los registros sin orden judicial de teléfonos inteligentes atendiendo a consideraciones de privacidad inherentes a la Cuarta Enmienda de la Constitución de los Estados Unidos. Cabe señalar, sin embargo, que la situación relativa a la seguridad y el cifrado de los teléfonos móviles puede ser mucho más compleja que aquella que únicamente gira en torno a los argumentos de privacidad y seguridad. Puede ser solo una cuestión de tiempo antes de que los magistrados del Tribunal Supremo de los Estados Unidos se enfrenten al mismo dilema a que se enfrentaría el gran número de países de todo el mundo que han reconocido el derecho a guardar silencio o el derecho a no incriminarse como uno de los principios de dignidad que una sociedad democrática suscribe. Esto se debe a que las propias características de un teléfono móvil que lo convierten en un archivo tan especial de datos personales, como se expone en la causa *Riley c. California*, también lo convierten en el instrumento más evidente que podría socavar total y efectivamente el derecho a guardar silencio, que ha sido reconocido de forma gradual en diversas jurisdicciones desde el siglo XVI y

que en los Estados Unidos se reconoce como la Quinta Enmienda. En pocas palabras, en muchas jurisdicciones de todo el mundo, pero no todas, una persona acusada tiene derecho a no inculparse permaneciendo en silencio durante los procedimientos penales incoados contra ella. Hay muy pocas excepciones o limitaciones a este derecho en países tan alejados como Alemania, Australia, Bangladesh, los Estados Unidos, la India, Nueva Zelandia, etc. Sin embargo, una orden judicial para acceder a los datos almacenados en un teléfono podría vulnerar efectivamente ese derecho. El acusado —hasta ahora no es un testigo competente que puede ser requerido a testificar— puede tener derecho a guardar silencio, pero su teléfono podría revelar mucho acerca de sus más íntimos pensamientos, intereses y acciones. En muchas jurisdicciones, el cónyuge o los familiares cercanos del acusado también pueden gozar de la misma condición de no ser testigos competentes que pueden ser obligados a testificar. Sin embargo, la mayoría de las personas afirmarían que sus teléfonos inteligentes saben mucho más acerca de ellos que sus cónyuges, por lo que cabe preguntarse si el teléfono inteligente seguirá siendo un testigo competente que pueda ser requerido a atestiguar aun cuando exista una orden judicial para acceder a su contenido. ¿Entonces, adónde debería llevarnos la lógica —y la coherencia lógica—?

26. En este momento, el Relator Especial sobre el derecho a la privacidad está señalando esta cuestión de los teléfonos inteligentes y otros dispositivos similares (incluidos implantes y tecnologías ponibles) como una cuestión que deberá ser objeto de debate en el futuro, posiblemente por parte de otros relatores especiales o en colaboración con ellos. En esta coyuntura preliminar, el Relator Especial no formula ninguna opinión o recomendación particular. En esta etapa, se trata simplemente de señalar un tema para su investigación ulterior como una cuestión que menoscaba en gran medida la privacidad, pero no solo es exclusivamente relevante para el derecho a la privacidad, sino también para otros derechos fundamentales, como el derecho a las garantías procesales en los procedimientos penales. Algunos podrían aducir que la conclusión lógica de *Riley c. California*, cuando se aplica al derecho a guardar silencio, que se distingue del derecho a la privacidad, implicaría que en la mayoría de los casos los teléfonos inteligentes de los acusados en procesos penales no deberían ser testigos a los que se les pueda requerir atestiguar —posición que luego también tendría importantes repercusiones en el derecho a la privacidad, en la medida en que sería sin duda un reconocimiento de los íntimos y privados que pueden ser los datos contenidos en el teléfono inteligente—.

27. El Reino Unido de Gran Bretaña e Irlanda del Norte, donde, irónicamente, los orígenes del derecho a guardar silencio pueden remontarse a más de 400 años, en realidad ha adoptado la posición de que la seguridad nacional o la represión del delito se impone a la privacidad o el derecho a guardar silencio cuando se trata de dispositivos electrónicos. Según lo dispuesto en los artículos 49 y 53 de la Ley de Regulación de las Facultades de Investigación de 2000, constituye un delito el no revelar la clave para acceder a los datos cifrados cuando se solicite (con una pena de 2 años de prisión, o de 5 años cuando se trate de casos de abuso sexual infantil). Así pues, en el Reino Unido, el teléfono inteligente no solo es un testigo competente que puede ser requerido a atestiguar, sino que, de no proporcionarse las claves del dispositivo, se correría el riesgo de ser condenado a una pena de prisión adicional. El caso de Apple contra el FBI difería ligeramente en que los acusados estaban en

realidad muertos y no había ninguna duda en cuanto a su culpabilidad, pero era necesario acceder al teléfono para tener una perspectiva más amplia de los hechos y la preparación del acto de terrorismo, así como de los colaboradores y las conexiones en lo que podría ser una red terrorista nacional o internacional. Sin embargo, el interés que ha suscitado el caso es justamente merecido por cuanto nos lleva al centro de los debates sobre la privacidad, la seguridad y el derecho a guardar silencio. Quizá el paso siguiente sea organizar un estudio en el punto de intersección del derecho a la privacidad y el derecho a guardar silencio. El Relator Especial consultará con la International Bar Association, colegios de abogados europeos y otros diversos interesados antes de formarse una opinión sobre si ha llegado el momento de proceder a una investigación en profundidad y si se precisan recomendaciones para la formulación de políticas con base empírica en esta esfera.

B. Conservación de datos, vigilancia masiva y aún más cifrado

28. Pese a las resoluciones de numerosos tribunales constitucionales nacionales y tribunales regionales de derechos humanos, el Relator Especial observa que existe una tendencia creciente por parte de los Gobiernos a promover leyes de vigilancia más invasivas, que prevén una vigilancia permanente masiva apenas disimulada de los ciudadanos.

29. Se sigue avanzando en este sentido con la aprobación de la tercera lectura del proyecto de ley de facultades de investigación en la Cámara de los Comunes del Reino Unido. Está previsto que el proyecto de ley continúe examinándose en la fase del Comité en la Cámara de los Lores en septiembre de 2016. El Relator Especial debe suponer que los lectores también están familiarizados con las críticas que formuló contra el proyecto de ley en su informe de 9 de marzo de 2016. La parte del proyecto de ley que se ocupa de la vigilancia y la piratería masivas sigue siendo objeto de escrutinio internacional. El Tribunal de Justicia de la Unión Europea resolverá sobre el asunto a raíz de la opinión expresada por el Abogado General del Tribunal, el 19 de julio de 2016, de que el procesamiento masivo solo es legal en los casos de delito grave, lo que constituye un uso mucho más limitado que el permisible en virtud del proyecto de ley. El proyecto de ley sigue siendo un campo minado para la privacidad, cuyo análisis minucioso exige diez veces el límite de 10.300 palabras que el presente informe debe respetar, pero, afortunadamente, diversos ministros del Parlamento, Liberty, The Law Society, el Open Rights Group y Privacy International están librando la batalla con valentía. Solo cabe esperar que el Gobierno del Reino Unido pulse el botón de pausa, escuche atentamente lo que el Tribunal Europeo de Derechos Humanos y el Tribunal de Justicia tienen que decir acerca de la vigilancia y permita que prevalezca la cordura. También sería conveniente que escuchara a algunos miembros de su propia Cámara de los Lores. Lord Paddick, ex Oficial Superior de Policía, ha arremetido contra las disposiciones del proyecto de ley relativas a los registros de conexión a Internet, diciendo que los registros de conexión a Internet —el único terreno virgen en el proyecto de ley— van a invadir la privacidad de personas inocentes. Sostiene más adelante que el carácter general de los registros de conexión a Internet es desproporcionado, en

vista de que el proyecto de ley permite a la policía acceder a estos datos personales de todos los usuarios de Internet en el Reino Unido sin orden judicial mediante⁸.

30. Poco importa que el proyecto de ley de facultades de investigación, para empezar, nunca debiera haberse propuesto en su forma actual ni presentado para su aprobación por la Cámara de los Comunes. El debate en la Cámara de los Lores hasta la fecha no ha sido alentador. Earl Howe, Ministro de Estado de Defensa y Jefe Adjunto de la Cámara de los Lores, dijo, el 13 de julio de 2016:

Que podía ser perfectamente lógico que el Gobierno colaborase con los proveedores de servicios de comunicaciones a fin de determinar si sería razonablemente factible adoptar medidas encaminadas a crear y mantener una capacidad técnica para eliminar el cifrado que se ha aplicado a las comunicaciones o los datos, a lo que añadió que los organismos encargados de hacer cumplir la ley y los organismos de inteligencia debían conservar la capacidad de exigir a los operadores de telecomunicaciones que eliminen el cifrado en determinadas circunstancias⁹.

31. Declaraciones como estas apuntan a una de entre cuatro opciones: a) el Ministro está siendo mal informado; b) el Ministro está siendo informado por personas que no entienden cómo funciona realmente el cifrado; c) el Ministro no entiende el informe; o d) el Ministro está tergiversando deliberadamente la situación ante la Cámara de los Lores. El Relator Especial no quiere creer que se trata de un caso de falsa declaración deliberada y, por lo tanto, hace un llamamiento al noble Lord y a todos sus colegas miembros de la Cámara de los Lores para que aborden la esencia de algunos hechos básicos. Quizá si los miembros de la Cámara de los Lores comprendieran los argumentos presentados por el Gobierno de los Países Bajos el 4 de enero de 2016 entenderían, entonces, por qué los intentos de legislar el desarrollo de un cifrado más débil son una mala idea y especialmente ridículos en la práctica. Entenderían que, lejos de ser perfectamente lógicas, esas propuestas resultan completamente absurdas. También entenderían por qué son ilusorias y distan mucho de la realidad declaraciones tales como que los encargados de hacer cumplir la ley y los organismos de inteligencia deben conservar la capacidad de exigir a los operadores de telecomunicaciones que eliminen el cifrado en determinadas circunstancias. En la mayoría de los casos, los organismos de inteligencia y encargados de hacer cumplir la ley no tienen capacidad alguna de exigir a los operadores de telecomunicaciones que eliminen el cifrado —o bien pueden pedirles que lo hagan hasta la saciedad— por la sencilla razón de que, en la mayoría de los casos, los operadores de telecomunicaciones carecen, de entrada, de esa capacidad. Si el Parlamento del Reino Unido estuviera lo suficientemente desencaminado para aprobar un acto legislativo tan absurdo, solo haría falta un esfuerzo muy pequeño para que una persona descargue una serie de algoritmos de cifrado o programas de comunicaciones cifradas producidos fuera del Reino Unido o los Estados Unidos, pero disponibles gratuitamente en Internet, y luego utilice

⁸ Cámara de los Lores del Reino Unido de Gran Bretaña e Irlanda del Norte, debate sobre el proyecto de ley de facultades de investigación de 27 de junio de 2016, vol. 773. Disponible en <https://hansard.parliament.uk/lords/2016-06-27/debates/1606278000466/InvestigatoryPowersBill>.

⁹ *Ibid.*, debate sobre el proyecto de ley de facultades de investigación de 13 de julio de 2016, vol. 774. Disponible en <https://hansard.parliament.uk/lords/2016-07-13/debates/16071337000437/InvestigatoryPowersBill>.

esos programas para comunicarse con otras personas con la intención de causar daño en el Reino Unido. Nada puede hacer un operador de telecomunicaciones en tales circunstancias, y un organismo de inteligencia de señales solo puede tratar de piratear el código.

32. Algunos miembros de la Cámara de los Lores entienden perfectamente el problema. Lord Strasburger lo expuso de manera muy sucinta:

Señaló que una característica del cifrado de extremo a extremo era que el proveedor no podía descifrar las claves, pues el cifrado era privado entre los usuarios en ambos extremos; que Earl Howe parecía dar a entender que los proveedores solo podían utilizar un cifrado cuyas claves fuera posible descifrar y, por consiguiente, no podía ser de extremo a extremo, de modo que la siguiente versión de iPhone de Apple pasaría, en teoría, a ser ilegal; y que, a su juicio, había mucho trabajo por hacer a ese respecto⁹.

El Relator Especial también lo cree, y sugeriría que gran parte de la labor que debe hacerse consistiera en alejar al Gobierno del Reino Unido de la ilusión de que puede ilegalizar efectivamente el cifrado de extremo a extremo o ponerlo fuera del alcance de las personas que viven en el Reino Unido. Esta propuesta se halla en el mismo nivel de razonamiento ilógico que tratar de prohibir todos los cuchillos por motivo de que en ocasiones podrían utilizarse para hacer daño, o prohibir los coches debido a que a veces se utilizan como vehículos de fuga. Además, los riesgos de seguridad que plantea el cifrado deliberadamente debilitado son muy desproporcionados respecto de los beneficios. Strasburger lo resumió:

Destacando que, como cualquier persona en la industria criptográfica lo dejaría claro, no se pueden conseguir las dos cosas a la vez; que el cifrado es seguro, o no lo es; y que no puede ser inseguro para un pequeño grupo de usuarios y seguro para el resto⁹.

Lord Paddick apuntó a un enfoque que sería más coherente con la jurisprudencia del Tribunal Europeo de Derechos Humanos expresada en fecha más reciente en la causa *Zakharov c. Rusia*, que establece que, en lugar de la facultad de obligar a una empresa a eliminar el cifrado de todo un servicio o tecnología, deberían usarse facultades alternativas y más específicas⁹. En la etapa actual, el Relator Especial solo puede preguntarse cuándo prevalecerá finalmente el sentido común —y no digamos ya el merecido respeto de derechos humanos fundamentales como la privacidad— en el debate del Estado sobre el tema.

33. Durante decenios, Alemania ha sido un excelente ejemplo de promoción de la protección de la privacidad en algunos ámbitos. En abril de 2016, el Tribunal Constitucional de Alemania se mantuvo fiel a esta tradición cuando dictaminó que las partes de una ley (“BKA-Gesetz”) que otorgaban facultades de vigilancia a la policía federal eran inconstitucionales, porque no tenían suficientes salvaguardias para garantizar un equilibrio entre los derechos de la persona a la intimidad y los intereses del Estado en la investigación de posibles delitos. El Tribunal declaró que algunas facultades, como la capacidad de realizar actividades de vigilancia por medio de conversaciones grabadas o fotografías, colocar escuchas telefónicas o llevar a cabo registros remotos de ordenadores, no tenían suficientes restricciones, como la posibilidad de revisión judicial, para garantizar que las

intromisiones en la intimidad de los ciudadanos alemanes estuvieran justificadas y fueran proporcionales¹⁰.

34. La supervisión democrática de los servicios de inteligencia de Alemania sigue siendo motivo de preocupación. El Relator Especial comparte las preocupaciones de Nils Muižnieks, Comisario para los Derechos Humanos del Consejo de Europa, y observa que sus conclusiones de octubre de 2015 no han sido refutadas. En particular, que:

Los problemas actuales relacionados con la supervisión eficaz de los servicios de inteligencia y seguridad en Alemania son la falta de recursos y de conocimientos especializados, el alcance de la supervisión de las telecomunicaciones, los problemas de coordinación, así como la falta de medios de defensa efectivos para las personas afectadas por la vigilancia de sus telecomunicaciones.

El Comisario está particularmente preocupado por la falta de recursos y conocimientos técnicos de los órganos de supervisión y su secretaría. A este respecto, la relación entre el número de supervisores y el número de personas sujetas a supervisión es especialmente elocuente: dos órganos de 13 miembros, que cuentan con el apoyo de una pequeña secretaría, se encargan de supervisar las actividades en que participan, en el caso del mayor organismo (BND), unos 6.000 miembros del personal¹¹.

El Relator Especial tiene la intención de dar seguimiento a esas preocupaciones en diversos foros, entre ellos HIOF2016, y, en el momento oportuno, abordarlas directamente con el Gobierno de Alemania.

35. El 28 de junio de 2016, el Gobierno de Alemania firmó un proyecto de ley sobre el Servicio Federal de Inteligencia (el Bundesnachrichtendienst o BND) que modificó varias leyes existentes que contenían disposiciones relativas a la vigilancia de ciudadanos no alemanes fuera de Alemania. El 8 de julio de 2016, el Parlamento aprobó la primera lectura del proyecto de ley. Se prevé que las dos lecturas restantes del proyecto de ley, incluida la votación final, puedan realizarse ya en el cuarto trimestre de 2016.

36. La primera observación que debe formularse a este respecto gira en torno a la cuestión de la nacionalidad, pues el proyecto de ley sigue haciendo distinciones entre ciudadanos alemanes y no alemanes. La forma en que ello refleja la realidad no ha quedado nada clara. La mayoría de los atentados terroristas perpetrados en Europa durante los últimos dos años y más fueron cometidos por ciudadanos de la Unión Europea, en la mayoría de los casos por ciudadanos del Estado donde se perpetró el atentado. Si el principal riesgo está ahí (es decir, en los ciudadanos del

¹⁰ Wenzel Michalski, "Dispatches: rare victory for privacy in Germany's 'war against terror'", Human Rights Watch, 27 de abril de 2016. Disponible en <https://www.hrw.org/news/2016/04/27/dispatches-rare-victory-privacy-germanys-war-against-terror>. <https://www.hrw.org/news/2016/04/27/dispatches-rare-victory-privacy-germanys-war-against-terror>

¹¹ Consejo de Europa, "Report by Nils Muižnieks, Commissioner for Human Rights of the Council of Europe: following his visit to Germany on 24 April and 4 to 8 May 2015", 1 de octubre de 2015. Disponible en https://www.ecoi.net/file_upload/1226_1447235185_commdh-2015-20-en.pdf. https://www.ecoi.net/file_upload/1226_1447235185_commdh-2015-20-en.pdf

propio Estado), ¿cuál es la verdadera utilidad de las leyes que discriminan entre los nacionales y los no nacionales? Especialmente teniendo en cuenta que, según lo dispuesto en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, toda persona tiene derecho a la privacidad, con independencia de su nacionalidad o ciudadanía, cabe preguntarse en qué medida pueden ser útiles y apropiados, y no digamos ya legales, esos tipos de disposiciones. El Sr. Muižnieks también observó esta anomalía y señaló que, según las autoridades, la protección que ofrece el artículo 10 de la Ley Fundamental no se extiende a las actividades fuera de Alemania, y se limita a los ciudadanos alemanes o a las actividades que se desarrollan en Alemania. Esta interpretación es tan inaceptable como cualquier pretensión en la legislación de otros países de que la protección de los derechos humanos fundamentales solo se limita a sus propios ciudadanos o residentes. De hecho, el Sr. Muižnieks señaló también lo siguiente:

Sin embargo, esta interpretación es controvertida, ya que el Tribunal Constitucional Federal resolvió en 1999 que la protección que ofrece la Ley Fundamental no se limita al territorio de Alemania, y que deben respetarse los derechos fundamentales, al menos cuando la información que se obtenga en el extranjero se procese en Alemania¹¹.

El nuevo proyecto de ley alemana desaprovecha una valiosa oportunidad para aclarar que el derecho a la privacidad y las salvaguardias correspondientes se aplican a las personas independientemente de su nacionalidad, ciudadanía o ubicación, o incluso si la vigilancia se lleva a cabo dentro o fuera de Alemania.

37. Además, el proyecto de ley alemana suscita muchas otras preocupaciones:

a) Especificación de la finalidad: las condiciones para la recopilación y el procesamiento de datos son vagas y demasiado amplias;

b) Vigilancia masiva: se autorizaría efectivamente la vigilancia masiva y selectiva de comunicaciones extraterritoriales entre ciudadanos no alemanes en los casos en que la interceptación de las comunicaciones se realice en Alemania. Si bien la vigilancia selectiva acorde con los criterios expuestos en *Zakharov c. Rusia* preocupa menos, la vigilancia masiva sigue siendo motivo de grave preocupación y, *prima facie*, es contraria a las normas establecidas en el derecho europeo;

c) La supervisión independiente: la nueva ley no contempla una supervisión judicial independiente adecuada;

d) El nivel de recursos de la supervisión de la vigilancia masiva propuesta en el proyecto de ley es irremediablemente insuficiente e inadecuado. La nueva ley prevé un comité de tres miembros, al que solo se le exige reunirse cuatro veces al año y que tal vez no tenga personal o recursos suficientes para supervisar las operaciones de vigilancia masiva, que, por su propia definición, son de amplio alcance. Esto deja al Relator Especial exactamente en la misma zona de preocupación expresada por el Sr. Muižnieks. Además, dado que el nombramiento de los miembros y la composición del comité corresponden al poder ejecutivo, la nueva ley no ayuda a que cobre fuerza la impresión de que la supervisión es independiente.

38. A la luz de lo que antecede, el nuevo proyecto de ley alemana lleva a pensar, *prima facie*, que las autoridades alemanas no han aprendido nada del informe de octubre de 2015 del Sr. Muižnieks. En lugar de ofrecer al Relator Especial una ley modelo que pueda servir de ejemplo de buenas prácticas en todo el mundo, el Gobierno de Alemania ha presentado algo que es más que decepcionante. Con sus múltiples defectos, el proyecto de ley de facultades de investigación del Reino Unido trataba al menos de subsanar en parte el deficiente régimen de supervisión criticado anteriormente por el Relator Especial y otros. Aunque dista de ser perfecto, el nuevo régimen de supervisión propuesto en el Reino Unido supondría una mejora con respecto a la situación anterior. No sucede así en Alemania, que, a menos que dé marcha atrás y cambie radicalmente de rumbo, da muestras de que vaya a asumir la posición que hasta ahora correspondía al Reino Unido como el país con el régimen de supervisión más débil del mundo occidental en proporción al tamaño de sus servicios de inteligencia.

39. Si bien el Relator Especial puede comprender la ansiedad que ha causado la reciente oleada de ataques en Alemania, sigue esperando que ese país asuma el liderazgo en la esfera de la protección de la privacidad y los datos y le ofrece, como en el caso del Reino Unido, trabajar con el Relator Especial para elaborar una nueva ley y crear un régimen de recursos de supervisión adecuado, que serviría de ejemplo de mejores prácticas en todo el mundo.

C. Mayor reconocimiento de la relación entre privacidad y personalidad

40. El Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) de México dictó un fallo muy interesante (Expediente PPD.0050/16) el 13 de julio de 2016, en el que se indica lo siguiente: “[E]s pertinente señalar que si bien el derecho a la protección de datos personales, conforme a su regulación constitucional, es un derecho autónomo de la protección de la vida privada, debe hacerse una interpretación amplia de ambos conceptos, en tanto que este último derecho implica una esfera en la que cualquier persona puede desarrollar libremente su personalidad”. Por lo tanto, en general, la protección de la vida privada abarca otros derechos y garantías específicas para el almacenamiento de la información, el acceso a datos personales, así como la reglamentación sobre la protección de las comunicaciones privadas, los nombres y la integridad física y moral.

IV. Conclusiones

41. En el primer año completo de mandato, el Relator Especial ha visitado 14 países durante 20 viajes realizados en el marco de sus actividades. Entre ellos cabe mencionar las visitas a países geográficamente tan distantes como Australia, el Brasil, los Estados Unidos y Nueva Zelandia, así como diez Estados europeos. Aunque técnicamente fueron visitas “oficiosas”, en muchas ocasiones incluyeron toda la gama de actividades que se realizan durante las visitas oficiales tradicionales del Relator Especial, en particular reuniones con ministros, funcionarios de ministerios, los servicios de inteligencia, los

organismos de supervisión, comisionados para la protección de datos, las fuerzas del orden, la sociedad civil y las principales empresas. En un gran número de casos, el Relator Especial fue recibido de manera muy positiva. Los próximos 12 meses también incluirán al menos 2 y posiblemente 3 visitas oficiales a los países, todas provisionalmente programadas, cada una en 3 continentes diferentes (África, América Latina y Asia).

42. El Relator Especial ha puesto en marcha un sistema de consultas estructuradas en todo el mundo. La sociedad civil, los particulares, los Gobiernos, las empresas y otros interesados han manifestado su interés en diversos temas relacionados con la privacidad dirigiéndose por escrito al Relator Especial o solicitando la celebración de reuniones, solicitudes que, en su mayoría, fueron atendidas. Estas reuniones han permitido al Relator Especial confeccionar listas de las partes interesadas en diversos sectores y utilizarlas para invitar a los interesados a las reuniones en todo el mundo. Las consultas estructuradas a menudo se celebran a puerta cerrada (a petición de los interesados), pero pueden incluir una combinación de invitados y personas que escriben solicitando asistir a un evento publicitado.

43. Además, el Relator Especial ha creado estructuras para seguir investigando y celebrando consultas mediante el establecimiento de cinco grupos de trabajo, cada uno correspondiente a una línea de acción temática definida en el primer conjunto de cinco prioridades: macrodatos y datos abiertos; seguridad y vigilancia; datos sanitarios; datos personales procesados por las empresas; y “una mejor comprensión de la privacidad”. Estos sentarán las bases para la elaboración de informes temáticos, que se espera comiencen a presentarse en el período 2017-2018. Esta metodología ha permitido al Relator Especial superar en parte las limitaciones de recursos recurriendo a una reserva mundial de expertos dispuestos a aportar sus conocimientos especializados con carácter voluntario y sin remuneración. No obstante, el Relator Especial seguirá buscando financiación externa, y acoge con agrado todas las formas de asistencia para llevar a cabo su mandato de manera adecuada.

44. El presente informe se ve limitado por el máximo arbitrario de palabras impuesto, y en él se han omitido observaciones sobre al menos una docena de esferas en las que el titular del mandato especial ha trabajado. Se espera que estas esferas se desarrollen más a fondo en futuros informes temáticos y genéricos.

45. Aunque está generalmente satisfecho con la colaboración obtenida hasta la fecha, el Relator Especial recomienda que un mayor número de Gobiernos colaboren con el mandato y, como otros Gobiernos han hecho durante el primer año de actividad, celebren consultas sobre los proyectos de ley relativos a la privacidad y esferas conexas como la vigilancia cuando estos se encuentren aún en una etapa temprana. Además, el Relator Especial alienta encarecidamente y valora en alto grado la participación en iniciativas organizadas por él, como IIOF2016, visitas oficiales a los países o diversas conferencias de mesa redonda, así como su facilitación.