Naciones Unidas A/HRC/31/64

Asamblea General

Distr. general
24 de noviembre de 2016
Español
Original: inglés

Consejo de Derechos Humanos
31er período de sesiones
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 el presente informe, presentado al Consejo de Derechos Humanos en virtud de su resolución 28/16, el Relator Especial sobre el derecho a la privacidad expone la concepción que tiene de su mandato, así como sus métodos de trabajo y un plan de trabajo trienal. En el informe también figura una reseña general de la situación en que se hallaba la privacidad a principios de 2016.

* El informe se presentó después del plazo límite para reflejar los acontecimientos más recientes.
** Los anexos del presente informe se distribuyen tal como se recibieron, en el idioma en que se presentaron únicamente.

GE.16-20847 (S) 061216 081216
1620847

Informe del Relator Especial sobre el derecho a la privacidad

Índice

I. Introducción

1. El Consejo de Derechos Humanos fijó el mandato del Relator Especial sobre la privacidad en su resolución 28/16, relativa al derecho a la privacidad en la era digital, en la que observó que los Estados debían garantizar el pleno cumplimiento de sus obligaciones en virtud del derecho internacional de los derechos humanos. El derecho a la privacidad es un derecho particularmente difícil de ejercer, pues el veloz desarrollo de la tecnología de la información no solo ofrece nuevas oportunidades de interacción social, sino que también suscita inquietudes sobre cómo elaborar adicionalmente ese derecho para hacer frente a los nuevos problemas.

2. En virtud de la resolución citada, el Relator Especial informará anualmente al Consejo y a la Asamblea General. En el presente informe, el Relator Especial expone sus métodos de trabajo (sección II), la situación en que se halla la privacidad en 2016 (sección III), sus actividades hasta la fecha (sección IV) y un plan de diez puntos con el que pretende esclarecer y elaborar adicionalmente el derecho a la privacidad en el siglo XXI (sección V). Por último, presenta sus conclusiones en la sección VI.

3. El presente informe se debería considerar un informe de carácter modesto y preliminar, dado que se ha elaborado apenas seis meses después del nombramiento del Relator Especial, que tuvo lugar el 1 de agosto de 2015. Por consiguiente y a pesar de los esfuerzos considerables de este, no ha habido tiempo suficiente para consultar con todos los interesados. La finalidad principal del presente informe es, por tanto, seleccionar una serie de cuestiones importantes, sin atribuirles un orden de prioridad necesariamente. Es de esperar que, una vez que haya tenido la oportunidad de escuchar el parecer de muchos más interesados de todo el mundo, el Relator Especial esté, en los próximos 12 meses (es decir, en enero de 2017), en unas condiciones mucho mejores de otorgar prioridad a las medidas que lo requieran. En el anexo I se exponen la concepción que tiene el Relator Especial de su mandato y los problemas que tiene previsto tratar.

II. Métodos de trabajo del Relator Especial

A. Supervisión de los países

4. Se está elaborando una base de datos sobre políticas, leyes, procedimientos y prácticas actuales, y poblándola con diversos informes y con las leyes pertinentes, lo que permitirá al Relator Especial determinar cuáles son las cuestiones de interés, así como las mejores prácticas, para luego divulgarlas.

B. Estudios temáticos: análisis y evaluación

5. En un mundo que se beneficia muchísimo de una Internet sin fronteras, las consultas del Relator Especial indican que hay un respaldo muy amplio a dos principios generales: las salvaguardias sin fronteras y los recursos jurídicos transfronterizos.

6. Esta preocupación por las salvaguardias para proteger la privacidad y por los recursos jurídicos para reparar los atentados contra esta subyace en cada uno de los estudios temáticos que ha realizado el Relator Especial sobre una serie de sectores en los que la privacidad parece correr riesgos elevados, los cuales se exponen a continuación. Está previsto que cada estudio dé lugar a un informe especial, en el que constarán las consultas, las interacciones y las observaciones que vaya habiendo.

1. La privacidad y la personalidad en las diversas culturas

7. Este estudio responde a la necesidad de adquirir una mejor comprensión de lo que es, o debería ser, la privacidad en las diversas culturas en 2016, de una manera que esté en consonancia con una era digital en la que Internet traspasa las fronteras. Al hacerse la pregunta de "¿por qué la privacidad?" y plantear la privacidad como un derecho habilitante en lugar de como un fin en sí mismo, el Relator Especial analiza la privacidad como un derecho que habilita el ejercicio del derecho fundamental y general desarrollar la propia personalidad de manera libre y sin trabas. Este análisis se realiza en estrecha cooperación con varias organizaciones no gubernamentales (ONG) y está previsto que sea el tema de una conferencia internacional importante, que se organizará en 2016. Este análisis se realiza también en un contexto más amplio: el de su relación con otros derechos fundamentales. Así pues, se prevé examinar la relación de la privacidad con la libertad de expresión y la libertad de acceso a la información de dominio público por, entre otros medios, la colaboración con otros Relatores Especiales de las Naciones Unidas. Ya se han entablado conversaciones con el Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, a fin de estudiar las oportunidades de colaboración en este ámbito durante 2016 y 2017.

2. Modelos de negocio en línea de las empresas y uso de los datos personales por parte de ellas

8. Durante los primeros 25 años de su existencia, la World Wide Web ha dado lugar al crecimiento espontáneo y, en gran medida, no reglamentado de empresas privadas, que en ocasiones se han convertido en entidades multinacionales que traspasan las fronteras nacionales y atraen clientes de todo el mundo. Una de las características principales de ese crecimiento ha sido la recopilación y el uso de datos personales; todas las búsquedas, todos los textos leídos, todos los correos electrónicos o cualquier otro tipo de mensaje, todos los productos comprados o los servicios contratados dejan centenares de miles de huellas electrónicas, que se pueden acumular para construir un perfil muy exacto de lo que le gusta o no le gusta a una persona, sus estados de ánimo, su solvencia económica, sus preferencias sexuales, su historial de salud y sus hábitos de compra, así como sus intereses y convicciones intelectuales, políticos, religiosos y filosóficos. En general, se suscita la pregunta de si ciertos proveedores de servicios en línea tienen derecho a investigar la conducta de las personas, a fin de garantizar una reparación justa. Este mapa de datos sobre el comportamiento de los consumidores, que es cada vez más detallado, ha hecho que los datos personales se conviertan en una mercancía. El acceso a esos datos, o su explotación, es actualmente uno de los mayores negocios del mundo, ya que produce unos ingresos que se calculan en centenares de miles de millones de dólares y se derivan, por lo general, de la publicidad personalizada. Muy a menudo se tiene la impresión de que, aunque los consumidores sean conscientes de los contenidos que exponen en línea deliberadamente, son mucho menos conscientes de la cantidad, la calidad y los usos específicos de los metadatos que producen cuando navegan, chatean, compran o realizan otras operaciones en línea. Los datos de que se dispone para trazar el perfil de las personas son actualmente varios órdenes de magnitud mayores que hace 25 años, pero no hay una comprensión cabal de la amplitud de los riesgos que entrañan para la privacidad el uso o el abuso de esos datos. Hay indicios de que la mercantilización de los datos personales, sobre todo en los sectores considerados sensibles tradicionalmente, como el sector del tratamiento de los datos médicos, ha aumentado hasta el punto de que una persona no es consciente de que esos datos se venden, o se revenden numerosas veces, ni otorga su consentimiento a ello. No hay suficientes pruebas para determinar con exactitud los riesgos inherentes a los datos presuntamente anonimizados, cuyo proceso de anonimización se puede desandar hasta llegar a identificar a la persona. Este atentado contra la privacidad podría entrañar numerosos riesgos para una persona, así como para su entorno social, sobre todo si se

accede a sus datos sin autorización y los que acceden son, por ejemplo, autoridades del Estado que desean adquirir poder o mantenerlo u organizaciones delictivas o sociedades mercantiles que obran ilegalmente. En la primera época de los ordenadores digitales, una de las preocupaciones principales era el uso de los datos personales por parte de los Estados y su capacidad de correlacionar datos de diversas fuentes para trazar un cuadro preciso de las actividades y el patrimonio de una persona. Sin embargo, en 2016 parece que son las empresas las que tienen muchos más datos que los Estados sobre las personas. Los ingentes ingresos derivados de la monetización de los datos personales hacen que no haya incentivos muy fuertes para cambiar el modelo de negocio en atención exclusivamente a las inquietudes respecto de la privacidad. En realidad, solo cuando, en los últimos tiempos, los riesgos para la privacidad han empezado a amenazar las posibilidades que tenía el modelo de negocio de producir ingresos, algunas empresas han adoptado un criterio más estricto y más favorable a la privacidad. Ahora parece conveniente abrir un debate global, fundamentado en la reunión de pruebas apropiadas, a fin de determinar qué tipo de política de información es la más adecuada para incrementar al máximo la protección de la privacidad de las personas en relación con los datos que recopilan sobre ellas las empresas, y minimizar los riesgos consecuentes. Será un debate en el que se tendrán en cuenta las ideas y las previsiones que los ciudadanos han expuesto en el párrafo 8. Es de esperar que en las consultas que empezaron en 2015 se dé cabida a las empresas que operan en línea en 2016, y está previsto celebrar una consulta pública muy amplia sobre este tema en 2017.

3. Seguridad, vigilancia, proporcionalidad y paz informática

9. La preocupación internacional por la seguridad siguió ocupando un lugar destacado en las actividades de 2015 y las de 2016. En el proceso de supervisión de países que ya se ha expuesto surgieron varios ejemplos de leyes que se estaban elevando urgentemente a los parlamentos nacionales para legalizar la aplicación, por parte de los servicios de seguridad e inteligencia y las fuerzas del orden de esos Estados concretos, de determinadas medidas que invadían la privacidad. En muchos de ellos, aunque lamentablemente no en todos, la introducción de esas medidas legislativas dio lugar a un debate público sobre las siguientes cuestiones:

a) La adecuación de los mecanismos de supervisión;

b) La distinción entre vigilancia específica y vigilancia a gran escala (o vigilancia masiva, como se la llama eufemísticamente en algunos países);

c) La proporcionalidad de esas medidas en una sociedad democrática;

d) La eficacia en función de los costos y la eficacia general de esas medidas.

10. La lucha contra el terrorismo y la delincuencia organizada, así como otros delitos a los que la sociedad es particularmente sensible, como la pedofilia, son los fines principales declarados de esas leyes. En esos debates se han aportado datos contradictorios que, a menudo, insinúan que las medidas de invasión de la privacidad, y sobre todo la vigilancia a gran escala, no mejoran la seguridad y que los fallos de los servicios de inteligencia se tienen que tratar por otros medios. El Relator Especial ha aplicado un programa de colaboración constante con las fuerzas del orden y los servicios de seguridad e inteligencia de todo el mundo para intentar comprender mejor sus intereses legítimos, reconocer cuáles son las mejores prácticas, que podrían divulgarse provechosamente, y determinar las políticas, las prácticas y las leyes de utilidad dudosa o que presenten un grado inadmisible de riesgo para la privacidad, tanto a nivel nacional como mundial. En algunos casos, este análisis que se está realizando se une, de manera casi indisoluble, a las cuestiones de la seguridad y el espionaje informáticos. Un pequeño pero creciente número de Estados tratan el ciberespacio como otro escenario bélico para una multitud de organismos de seguridad e inteligencia; por el momento, parece que no están dispuestos a colaborar entre sí —y en

ocasiones con el Relator Especial— para tratar de esas cuestiones, lo que, como es lógico, influye directamente en la privacidad de los ciudadanos, con independencia de su nacionalidad. Aunque no sea necesariamente el objetivo primordial de las medidas de seguridad y espionaje informáticos, a menudo el ciudadano común se puede ver atrapado en el fuego cruzado y sus datos personales y sus actividades en línea pueden acabar siendo vigilados en nombre de la seguridad nacional, de manera innecesaria, desproporcionada y excesiva. Aparte de disponer de los datos procedentes de la labor investigadora que ha realizado expresamente en cumplimiento de su mandato, el Relator Especial tiene la fortuna de poder acceder a la cuantiosa base de datos que le proporcionan las investigaciones colaborativas independientes, tanto anteriores como actuales, en la esfera de la seguridad, especialmente las financiadas por la Unión Europea[a]. El Relator Especial estudia esta esfera en cuatro aspectos principales: a) capacidades de vigilancia del Estado que sean proporcionadas en su ámbito de aplicación y estén debidamente limitadas mediante salvaguardias legislativas, procedimentales y técnicas, entre ellas unos mecanismos de supervisión sólidos; b) concentración en la vigilancia específica, en lugar de la vigilancia a gran escala; c) acceso de las fuerzas del orden y los servicios de seguridad e inteligencia a los datos personales que estén en posesión de las empresas privadas y otras entidades que no sean públicas; y d) la insistencia renovada en la paz informática. El Relator Especial cree firmemente que el ciberespacio corre el riesgo de ser destruido por la guerra y la vigilancia informáticas y que los Gobiernos y otros interesados deberían trabajar en pro de la paz informática. En ese sentido al menos, la protección de la privacidad también forma parte de la aspiración a lograr esa paz. Y, de esta manera, el ciberespacio puede convertirse verdaderamente en un espacio digital en el que la persona pueda esperar que se respeten su privacidad y su seguridad, un espacio pacífico que no corra peligro constante debido a las actividades de algunos Estados y a las amenazas que entrañan los terroristas y la delincuencia organizada.

4. Análisis de datos abiertos y macrodatos: su repercusión en la privacidad

11. Una de las cuestiones más importantes de la política y la gobernanza de la información en el segundo decenio del siglo XXI es la de determinar el equilibrio apropiado entre, por un lado, el uso de datos en beneficio de la sociedad según los principios de los datos abiertos y, por otro, los principios establecidos hasta la fecha para proteger los derechos fundamentales, como la privacidad, la autonomía y el libre desarrollo de la propia personalidad. En el anexo II figura una exposición más detallada de los intereses del Relator Especial en esta esfera.

5. Genética y privacidad

12. El Relator Especial observa que aproximadamente un cuarto de los Estados Miembros han creado bases de datos nacionales con el ADN de delincuentes. Las bases forenses de datos de ADN pueden servir de mucha ayuda para resolver delitos, pero también suscitan inquietudes en materia de derechos humanos, como la posibilidad de que se abuse de la vigilancia gubernamental (por ejemplo, para identificar a familiares y descartar paternidades) y de que se produzcan denegaciones de justicia. Además, se prevé que el uso de bases de datos de ADN con fines administrativos, por ejemplo para documentos de identidad o control de la inmigración, aumente exponencialmente. Por otra parte, en los próximos años, es probable que se avance hacia la creación de una base de datos de ADN de todos los ciudadanos. En lo que constituye una repetición de las inquietudes que surgieron en el decenio de 1990 acerca del uso de los datos genéticos en el sector de los seguros, se insinúa que la medicina personalizada inducirá a muchas personas

[a] Cabe citar proyectos como CONSENT, SMART, RESPECT, SiiP, INGRESS, E-CRIME, EVIDENCE, MAPPING, CITYCoP y CARISMAND.

a ofrecer voluntariamente la totalidad de su genoma humano a la industria de la salud. Dadas esas y otras preocupaciones, hay una necesidad creciente de plantear un debate público más amplio en un momento en el que las bases de datos de ADN se extienden cada vez más por el mundo. El Relator Especial pretende seguir colaborando en proyectos destinados a fijar unas normas internacionales de derechos humanos para las bases de datos de ADN, seleccionando las mejores prácticas e implicando en el debate a los especialistas, los encargados de formular políticas y la opinión pública. Es de esperar que esa colaboración ayude a formular unas directrices sobre mejores prácticas, que se habrán de elaborar con la aportación y las opiniones de los agentes de la sociedad civil.

6. Privacidad, dignidad y reputación

13. Es posible que la preocupación por la seguridad y la vigilancia haya desviado la atención de otras preocupaciones que comparten muchos ciudadanos sobre el riesgo que corren su privacidad, dignidad y reputación en Internet. El advenimiento de la era digital significa que los medios han evolucionado y cambiado en comparación con lo que eran en los dos últimos decenios, especialmente en el sentido de que Internet ha permitido a ciudadanos normales que carecían de una formación académica en periodismo publicar contenidos textuales, de audio y de vídeo a su gusto y a cualquier hora del día. Esa novedad ha dado poder a los ciudadanos en muchos aspectos, sobre todo en las situaciones en que pueden utilizarla para eludir la censura u otros obstáculos o en que las tecnologías facilitan la libertad de expresión de una manera que fomenta la democracia en la sociedad. Por otro lado, este fenómeno de los ciudadanos que son, a la vez, periodistas y blogueros en un mundo mediático que se halla en rápida evolución, unido al uso tan extendido de las redes sociales, ha suscitado la preocupación general de que se está abusando del derecho a la libertad de expresión, lo que repercute negativamente en otros derechos humanos fundamentales, como la privacidad y la dignidad. En las investigaciones llevadas a cabo en los últimos cinco años se ha subrayado la creciente preocupación de los ciudadanos respecto de la facilidad con la que se pueden atacar y destruir su buen nombre y su reputación en Internet, así como la sensación de impotencia que sienten muchos ciberciudadanos cuando intentan obtener salvaguardias y reparación en casos de difamación o de invasión de su privacidad. El Relator Especial desearía colaborar con el Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, con la sociedad civil y con otros organismos de las Naciones Unidas, como la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura, con miras a estudiar salvaguardias concretas de la privacidad, la dignidad y la reputación de la persona en Internet, así como recursos jurídicos para reparar los atentados contra ellas. Como ocurre con otros de los estudios temáticos ya enunciados, la relación entre la privacidad y la gobernanza de Internet sigue siendo una de las cuestiones de fondo recurrentes que también atañen a la privacidad, la dignidad y la reputación.

7. Biometría y privacidad

14. Del estudio de las investigaciones actuales se desprende que ha habido un gran incremento del interés por usar la biometría con diversos fines, que van desde las labores policiales hasta el acceso personal a dispositivos móviles. Y, así, la identificación de voz, los escáneres de retina, el reconocimiento de la manera de caminar y de la cara y la tecnología de obtención de huellas digitales normales y huellas digitales subcutáneas son solo unos cuantos ejemplos de las muchas tecnologías digitales que se están desarrollando e implantando, con diversos fines, en el segundo decenio del siglo XXI. El Relator Especial pretende seguir cooperando con los investigadores biométricos, así como con las fuerzas del orden, los servicios de seguridad e inteligencia y la sociedad civil, a fin de prever salvaguardias y recursos jurídicos apropiados para el uso de esos dispositivos biométricos.

C. Denuncias individuales

15. El Relator Especial ha recibido, y probablemente seguirá recibiendo, sobre todo a medida que su mandato se conozca más ampliamente, denuncias de presuntas vulneraciones del derecho a la privacidad presentadas por particulares y agentes de la sociedad civil. Se hace un seguimiento de estas denuncias manteniendo correspondencia con los denunciantes y las autoridades gubernamentales competentes. Esta comunicación de seguimiento se realiza con arreglo a la metodología que emplean los titulares de mandatos de procedimiento especiales, que tiene por objeto aclarar las denuncias presentadas, determinar los hechos y, en su caso, formular recomendaciones para que se adopten medidas rectificativas. Esta comunicación también puede consistir en reuniones en línea o en persona, según proceda. Cuando las pruebas que se hayan recibido justifiquen una atención particular o urgente y las formas normales de comunicación no resulten apropiadas, el Relator Especial podrá estudiar la conveniencia de expresar públicamente su preocupación.

D. Actividades conjuntas

16. El Relator Especial recibe solicitudes periódicas para que realice, e inicie en ocasiones, actividades conjuntas con otros relatores especiales. Los detalles de esas actividades se publican aparte en el informe de comunicaciones, en la sección de procedimientos especiales.

17. Al 5 de marzo de 2016, solo se había dispuesto de tiempo para reunir, en alguna de las categorías que se han citado en los párrafos anteriores, datos empíricos suficientes como para participar en dos actividades conjuntas. Sin embargo, está previsto combinar la información que se haya reunido de cada categoría para crear la base de datos empíricos que se requiere para que el Relator Especial dialogue y coopere con los Estados pertinentes, por ejemplo mediante comunicaciones, visitas y otras fórmulas de cooperación.

E. Construcción de puentes y política de colaboración

18. El Relator Especial ha utilizado su mandato para continuar y ampliar la labor que se había llevado a cabo anteriormente de construir puentes con los interesados y entre ellos, lo que ha dado lugar a una política de colaboración permanente con todo tipo de interesados, entre ellos representantes de los gobiernos y ministros, en sus capitales o en reuniones bilaterales en foros internacionales; reuniones con diversas autoridades de protección de datos y privacidad, en particular con el Presidente del Grupo de Trabajo del Artículo 29 de la Unión Europea y el Presidente del Comité Consultivo del Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal del Consejo de Europa; debates con órganos de normalización técnica como la Unión Internacional de Telecomunicaciones (UIT) y el Instituto de Ingenieros Electricistas y Electrónicos; reuniones de análisis en profundidad con agentes de la sociedad civil, individuales o de grupo, y reuniones con especialistas en derechos humanos u otros funcionarios de las misiones permanentes con sede en Ginebra. Esta lista es meramente ilustrativa y no está completa. Se reciben, casi a diario, invitaciones para pronunciar discursos inaugurales, participar en mesas redondas y conferencias y reunirse con miembros de la sociedad civil. Aunque se han aceptado algunas de esas invitaciones, sobre todo las que guardaban relación directa con los siete estudios temáticos ya expuestos, otras se han tenido que declinar, sobre todo cuando las limitaciones de tiempo o de presupuesto impedían aceptarlas. Uno de los muchos resultados que ha dado esa política de colaboración ha sido la aprobación de una resolución en la que se formaliza la cooperación

con las autoridades de protección de datos y privacidad[b], en la Conferencia Internacional de Autoridades de Protección de Datos y Privacidad.

III. La privacidad a principios de 2016

A. Definición y comprensión

19. Aunque el concepto de "privacidad" exista en todas las sociedades y culturas —y esto haya sido así a lo largo de la historia de la humanidad—, no hay una definición vinculante y universalmente admitida de él[c]. Para comprender mejor el derecho a la privacidad hay que estudiarlo desde dos perspectivas diferentes. En primer lugar, hay que estudiar qué es lo que abarca el núcleo positivo de este derecho. En segundo lugar, hay que plantearse la pregunta de cómo delimitar ese derecho mediante una definición negativa. Sin embargo, estas dos tareas están pendientes de ejecución.

20. Como reafirmó el Consejo de Derechos Humanos en su resolución 28/16, el artículo 12 de la Declaración Universal de Derechos Humanos y el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos forman la base del derecho a la privacidad en el derecho internacional de los derechos humanos. Si se les suman otros instrumentos jurídicos nacionales e internacionales, como constituciones y leyes pertinentes, se llega a la conclusión de que en todo el mundo hay un marco jurídico de envergadura considerable que podría servir para proteger y promover la privacidad. No obstante, la utilidad de ese marco jurídico se ve gravemente menoscabada por la falta de una definición de la privacidad acordada y admitida internacionalmente. Aun cuando 193 naciones suscribieran el principio de protección de la privacidad, ello serviría de muy poco si esas naciones no comprendieran claramente qué es lo que han acordado proteger.

21. La falta de una definición de la privacidad acordada y admitida internacionalmente no es el único problema importante que afronta el Relator Especial. Aun cuando los redactores de todos los instrumentos jurídicos pertinentes hubieran incorporado en ellos una definición tal, aún habría que considerar las dimensiones temporales, geográficas, económicas y tecnológicas de la cuestión. El transcurso del tiempo y la repercusión de la tecnología, sumados a las distintas tasas de desarrollo económico y de implantación de tecnologías en puntos geográficos distintos, pueden requerir que los principios jurídicos fijados hace 50 años (cuando se aprobó el Pacto Internacional de Derechos Civiles y Políticos) o incluso hace 35 años (por ejemplo, cuando se aprobó el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal), por no hablar de los que se fijaron hace 70 años (en la Declaración Universal de Derechos Humanos), se reexaminen, se reelaboren y, quizá, se suplementen y complementen, para adaptarlos mejor a las realidades de hoy en día.

22. Dadas la falta de una definición universalmente convenida de la privacidad y las consideraciones temporales, geográficas, económicas y tecnológicas enunciadas, es evidente que hay que llegar a comprender lo que significa la privacidad para las distintas personas que se hallan en distintos lugares y circunstancias en todo el planeta. Por tanto, el

[b] Aprobada en la Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, el 27 de octubre de 2015, en Ámsterdam. Se puede consultar en https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Cooperation-with-UN-Special-Rapporteur-on-the-Right-to-Privacy.pdf.

[c] Véase un análisis mucho más detallado del estudio que ha realizado el Relator Especial sobre la existencia y las dimensiones temporales, geográficas y espaciales de la privacidad a lo largo de los milenios, en Joseph A. Cannataci, ed., *The Individual and Privacy*, volumen I (Oxford, Ashgate, 2015).

Relator Especial estima, a primera vista, que esta empresa es no solo una tarea de importancia fundamental sino también una prioridad.

23. En algunas culturas, el debate sobre la privacidad lleva aparejado un debate sobre el aborto. Sin entrar en lo bien o mal fundado que se halle ese planteamiento y con ánimo de despejar cualquier duda, el Relator Especial afirma que, en esta etapa preliminar de su mandato, se concentrará en la privacidad de la información. Se concentrará en la función y el papel que desempeña la privacidad en cuanto a determinar los flujos de información en la sociedad y sus consiguientes repercusiones en el desarrollo de la personalidad individual. También se ocupará de cuestiones relacionadas, como la distribución del poder y la riqueza dentro de la sociedad. No obstante, cuando se abordan así todas esas cuestiones, queda claro que no es exclusivamente la privacidad lo que influye en el flujo de información en la sociedad, sino que también influyen otros derechos, como la libertad de expresión y la libertad de acceso a la información de dominio público. Todos estos derechos son importantes y la concentración en uno de ellos no debería menoscabar la importancia y la protección de los demás. Considerar los derechos en su conjunto, cuando sea posible, es más productivo que considerarlos como contrarios entre sí. Así pues, en puridad, no resulta provechoso hablar de "privacidad frente a seguridad" sino que hay que hablar de "privacidad y seguridad", dado que ambas son necesarias. Se puede interpretar que ambos derechos son derechos habilitantes, y no fines en sí mismos. La seguridad es un derecho que habilita para ejercer el derecho general a la vida y, por su parte, cabe considerar la privacidad como un derecho habilitante en el seno de la compleja red general de flujos de información de la sociedad, que son de importancia fundamental para que los individuos tengan la autonomía y la capacidad para determinar sus opciones y elegir entre ellas de manera informada, a medida que desarrollan su personalidad a lo largo de la vida.

24. Al abrir el debate sobre lo que es y debería ser la privacidad, el Relator Especial desea concentrarse en los aspectos fundamentales y evitar que el debate se desvíe hacia las diferencias locales o culturales, tanto supuestas como reales, que constituyen la periferia de la privacidad, en lugar de ceñirse al núcleo firme de valores de la privacidad que, en última instancia, tal vez gocen de consenso universal. Para ayudar a mantener un debate desprejuiciado y bien estructurado sobre esos aspectos fundamentales, el Relator Especial pretende, con cierto grado de provocación, plantear que el derecho a la privacidad es un derecho habilitante, y no un fin en sí mismo. Varios países del mundo han reconocido la existencia de un derecho fundamental y general a la dignidad y al desarrollo de la propia personalidad de manera libre y sin trabas. Países tan alejados geográficamente como el Brasil y Alemania han incorporado ese derecho a su constitución, y el Relator Especial sostiene lo siguiente: a) que tal derecho a la dignidad y al desarrollo libre y sin trabas de la propia personalidad se debería considerar universalmente aplicable; y b) que los derechos ya reconocidos, como los derechos a la privacidad, la libertad de expresión y la libertad de acceso a la información, constituyen un trío de derechos habilitantes y que la mejor manera de tratarlos es considerar su capacidad de habilitar a un ser humano para desarrollar libremente su personalidad. El planteamiento de la privacidad o, mejor dicho, de la pregunta "¿por qué la privacidad?" en el ámbito de un debate más amplio sobre el derecho fundamental a la dignidad y al desarrollo libre y sin trabas de la propia personalidad refleja las realidades de la vida en la era digital. Este planteamiento debería ayudar a todos los participantes en el debate, con independencia del país o la cultura de los que provengan, a concentrarse en los aspectos fundamentales del desarrollo de la propia personalidad y en la clase de vida que querrían ayudar a proteger mediante la privacidad, en lugar de perder demasiado tiempo en decidir qué tradiciones en materia de privacidad de una cultura determinada habría que tratar, defender o promover.

25. Como se verá, en muchos casos, el debate sobre la privacidad no se puede desgajar, en esencia, del debate sobre el valor de la autonomía o el libre albedrío. Este último término ha sido objeto de largos debates y, por lo que respecta a su relación con los derechos a la

privacidad y al desarrollo de la personalidad, ha dado lugar en Alemania, a partir de 1983, al derecho constitucional al "libre albedrío informativo". Hay que ahondar en el atractivo y la validez de este concepto en un debate mundial sobre cuál sería la interpretación óptima del derecho a la privacidad en 2016; posiblemente, en el ámbito de un debate sobre la protección y la promoción del derecho fundamental a la dignidad y al desarrollo libre y sin trabas de la propia personalidad.

26. El trío de derechos habilitantes ya mencionados —la privacidad, la libertad de expresión y la libertad de acceso a la información— existía antes de la llegada de las tecnologías digitales, al igual que el derecho a la dignidad y al desarrollo libre y sin trabas de la propia personalidad. Sin embargo, la tecnología digital ha tenido repercusiones inmensas en esos derechos, tanto en el mundo físico (por ejemplo, con las tarjetas de crédito, la identificación por radiofrecuencia y otros sistemas electrónicos) como en el mundo digital, donde, hoy en día, los ciberciudadanos producen un número asombrosamente mayor de paquetes de datos sobre sí mismos que el que producían hace dos decenios, antes de que se hubieran conectado en línea. Los dispositivos móviles y las tecnologías convergentes, como los teléfonos móviles inteligentes —en los que convergen la telefonía, Internet y la fotografía— dan lugar a un nuevo estilo de vida, nuevas comodidades y nuevas expectativas en materia de utilidad y privacidad.

27. Asimismo, la repercusión de las nuevas tecnologías puede obligarnos a reconsiderar las distinciones entre privacidad individual y privacidad colectiva, así como las expectativas de privacidad en los espacios públicos y privados, en el ámbito de la dignidad y el ejercicio libre y sin trabas de la propia personalidad.

B. Observaciones iniciales de 2015 y 2016

28. Al Relator Especial le resulta difícil escoger cuáles fueron los sucesos más importantes en materia de privacidad en el período transcurrido desde que asumió su mandato, habida cuenta, sobre todo, de que no ha dispuesto de los recursos necesarios para llevar a cabo una investigación rigurosa de esos sucesos. Además, el Relator Especial no desea minimizar el importante papel que han desempeñado los agentes de la sociedad civil, como Privacy International y sus filiales, que durante casi 20 años han organizado los premios "Gran Hermano"[d], con los cuales han arrojado luz sobre los usos de la privacidad y los abusos contra ella. Por otro lado, el Relator Especial desea elogiar las buenas prácticas, las leyes, los fallos judiciales y también las ideas que podrían favorecer y acrecentar la protección de la privacidad. Por tanto, desea señalar a la atención del Consejo de Derechos Humanos, sin que la lista sea exhaustiva y enumerándolos en un orden aleatorio, los siguientes fenómenos importantes.

1. Moderación prudente: la negativa de los Países Bajos y los Estados Unidos de América a permitir puertas traseras en las comunicaciones

29. Se debería felicitar a los Gobiernos de los Países Bajos y los Estados Unidos de América por la moderación que han demostrado al negarse a permitir que se usen las leyes para introducir puertas traseras en las comunicaciones. El 4 de enero de 2016, el Gobierno de los Países Bajos anunció su oposición oficial a la incorporación de puertas traseras en los productos de cifrado. En un documento en el que exponía su postura[e], publicado por el Ministerio de Seguridad y Justicia y firmado por los ministros de seguridad y economía, el Gobierno afirmó que no era apropiado, en aquel momento, adoptar medidas jurídicas

[d] www.bigbrotherawards.org.

[e] Se puede consultar en www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2016Z00009&did=2016D00015 (se accedió a este sitio web el 23 de agosto de 2016).

restrictivas contra el desarrollo, la disponibilidad y el uso del cifrado en los Países Bajos. Se llegó a esa conclusión al final de cinco páginas en las que se habían expuesto los argumentos a favor de reforzar el cifrado y los contraargumentos a favor de permitir que las autoridades accedieran a la información. Si se introdujera, en un producto de cifrado, un dispositivo técnico que permitiera a las autoridades acceder a los archivos cifrados, estos archivos también serían más vulnerables a los delincuentes, los terroristas y los servicios de inteligencia extranjeros. Dicha medida podría tener consecuencias indeseables para la seguridad de la información que se comunicara y almacenara, y para la integridad de los sistemas de tecnología de la información y las comunicaciones, que son cada vez más importantes para el funcionamiento de la sociedad.

30. La postura del Gobierno de los Países Bajos parece ser más definida que la del Gobierno de los Estados Unidos, que se le adelantó unos tres meses. A principios de octubre de 2015, el Director del Buró Federal de Investigaciones, James Comey, Jr., declaró, en el testimonio que dio en el Capitolio, que el Gobierno no era partidario, por el momento, de presionar para que se aprobara una normativa que obligara a las empresas a descifrar los datos de los clientes. Una cuestión más preocupante, que salió a la luz en la reciente demanda contra Apple, es que el Gobierno de los Estados Unidos seguirá intentando persuadir a las empresas que han optado por cifrar los datos de sus clientes para que ideen una manera de que el Gobierno pueda averiguar, de todos modos, los datos de las personas cuando los necesiten en investigaciones criminales o de atentados terroristas. La postura del Relator Especial sobre este caso se ha expuesto de manera general, si bien independiente, en la declaración formulada por el Alto Comisionado de las Naciones Unidas para los Derechos Humanos el 4 de marzo de 2016[f]. Resultan alentadores los últimos comentarios emitidos por el Secretario de Defensa de los Estados Unidos, Ashton Carter, que declaró que un cifrado fuerte era esencial para la seguridad de la nación. En el discurso que pronunció ante un público compuesto por especialistas del sector tecnológico el 2 de marzo de 2016, dijo que no creía en las puertas traseras ni en los programas de cifrado que dejaban aberturas para que personas ajenas a esos programas leyeran los archivos codificados en clave. Esta postura concuerda con las declaraciones que formuló en octubre de 2015[g], y habría que alentarla y afianzarla.

2. El principio del fin judicial de la vigilancia a gran escala: la cuestión de fondo

31. El 6 de octubre de 2015, el Tribunal de Justicia de la Unión Europea dictó sentencia en el caso de *Maximillian Schrems c. Data Protection Commissioner* (Supervisor Europeo de Protección de Datos). El Tribunal declaró nula la decisión de la Comisión Europea en virtud de la cual se había instituido el marco denominado "de puerto seguro" y que se basaba en la directiva 95/46/EC. El Relator Especial desea destacar la que probablemente sea una de las partes más importantes de esa sentencia, en la medida en que ha ratificado (y sentado) un precedente:

> 94. En particular, se debe considerar que una normativa que permite a las autoridades públicas acceder de forma generalizada al contenido de las comunicaciones electrónicas lesiona el contenido esencial del derecho fundamental al respeto de la vida privada garantizado por el artículo 7 de la Carta…

32. Sin duda, se suscitará cierto debate sobre el significado preciso de "acceder de forma generalizada", y aquí el Tribunal se refiere claramente al contenido de las comunicaciones en contraposición a los metadatos, pero será interesante ver qué ley europea que legitime la vigilancia a gran escala, si es que llega a haberla, pasará la prueba de ese criterio si el

[f] Véase www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=17138&LangID=E.

[g] Véase http://europe.newsweek.com/us-defense-secretary-ashton-carter-doesnt-believe-encryption-backdoors-432811?rm=eu.

Tribunal se inclina por seguir aplicándolo estrictamente. Sin embargo, la ambigüedad queda despejada, al menos parcialmente, cuando se lee la sentencia del caso *Schrems* junto con la del caso *Zakharov*, que se expone más adelante y que constituye derecho europeo y se aplica como derecho en otros Estados miembros del Consejo de Europa.

3. La importancia de disponer de recursos jurídicos: cuestiones de ejecución y de procedimiento

33. Remitiéndose, una vez más, al caso *Schrems*, el Relator Especial celebra que el Tribunal de Justicia se haya convertido en un foro para personas como el demandante, que abrió el caso como persona preocupada por las consecuencias que pudiera tener el desarrollo de la moderna tecnología de la información en su dignidad de ser humano en una sociedad democrática. El que los particulares tengan la oportunidad de exponer sus argumentos y defender sus derechos ante una institución pública supranacional, poniendo en entredicho las relaciones de poder existentes, es esencial para adquirir un conocimiento que permita mejorar el bienestar de nuestra sociedad y que sea coherente con el desarrollo de un derecho internacional de los derechos humanos. La existencia de esos mecanismos es absolutamente indispensable para proteger los derechos humanos y restaurar la confianza en el uso de la tecnología por los Estados y otras instancias.

34. Lo anterior constituye el anuncio de una nueva transformación de la sociedad y apunta a que los derechos se tienen que respetar y reforzar en todas partes, no solo en el lugar donde se hallen los servidores.

35. La sentencia del Tribunal de Justicia también demuestra el valor añadido de los planteamientos normativos regionales, que pueden servir, en el futuro, para promover unos instrumentos jurídicos participativos, que se elaboren contando con la opinión de los ciudadanos y tengan una aplicación más amplia en todo el mundo.

4. La mera existencia de una medida de vigilancia secreta atenta contra el derecho al respeto de la vida privada

36. La Gran Sala del Tribunal Europeo de Derechos Humanos, en su sentencia de 4 de diciembre de 2015 sobre el caso *Roman Zakharov c. Rusia*[h], dictaminó, por unanimidad, que el sistema ruso de interceptación de comunicaciones de teléfonos móviles atentaba contra el artículo 8 del Convenio para la Protección de los Derechos Humanos y de las Libertades (Convenio Europeo de Derechos Humanos). Además, lo que es muy interesante es que el Tribunal admitió que, si se cumplían ciertas condiciones, un demandante podría declararse víctima de una infracción del artículo 8 por la mera existencia de una medida secreta de vigilancia. Y quizá lo más importante sea la declaración por la cual el Tribunal ilegalizó los sistemas de vigilancia a gran escala de una manera aún más explícita que la del Tribunal de Justicia en el caso *Schrems*:

> 270. El Tribunal estima que el modo de funcionamiento del sistema de vigilancia secreta de Rusia otorga a los servicios de seguridad y a la policía los medios técnicos para eludir el procedimiento de autorización e interceptar cualquier comunicación sin autorización judicial previa. Si bien nunca se puede, con independencia de cuál sea el sistema, descartar completamente la eventualidad de que un funcionario carente de honradez, negligente o con celo excesivo cometa irregularidades (*Klass y otros*, antecitado, párr. 59), el Tribunal estima, no obstante, que un sistema como el ruso, que permite a los servicios secretos y a la policía interceptar directamente las comunicaciones de cualquier ciudadano sin imponerle la

[h] *Roman Zakharov c. Rusia* [GC], 4 de diciembre de 2015, núm. 47143/06, *Reports of Judgments and Decisions*.

obligación de presentar una autorización de interceptación al proveedor de los servicios de comunicación o a quien corresponda, es particularmente susceptible de abuso. La necesidad de disponer de garantías contra las arbitrariedades y los abusos resulta, así pues, particularmente fuerte.

37. En esa sentencia se fija un criterio de referencia muy importante al insistirse en los requisitos de la sospecha razonable y de la autorización judicial previa, así como en la naturaleza inadmisible de "un sistema…, que permite a los servicios secretos y a la policía interceptar directamente las comunicaciones de cualquier ciudadano sin imponerle la obligación de presentar una autorización de interceptación". Este sería, pues, el criterio por el cual se debería medir toda ley vigente de vigilancia o toda nueva ley que se propusiera en cualquier país europeo. Asimismo, el Relator Especial observa con grave preocupación diversos informes sobre una decisión de la Duma rusa (el Parlamento) que permitiría anular las sentencias del Tribunal Europeo de Derechos Humanos[i]. Si esos informes son ciertos, esa decisión podría, en la práctica, suprimir unos recursos jurídicos muy importantes de que disponen los ciudadanos de los países que hayan ratificado el Convenio Europeo de Derechos Humanos, en particular los recursos contra la vulneración del derecho al respeto de la vida privada. El Relator Especial invita al Gobierno de la Federación de Rusia a que lo ayude a verificar esos informes con más precisión, estudiar la ley en cuestión más a fondo para entender sus matices y, en caso de que los informes resulten ser exactos en esencia, persuadir a la Duma de que derogue la ley de 4 de diciembre de 2015 y restituya, así, la eficacia de los recursos jurídicos de que disponen los ciudadanos rusos al amparo del Convenio Europeo de Derechos Humanos, en particular los recursos que pueden interponer contra el Estado cuando se lesione su derecho a la privacidad.

5. El proyecto de ley de potestades de investigación del Reino Unido de Gran Bretaña e Irlanda del Norte

38. Merecen reconocimiento las tres comisiones parlamentarias del Reino Unido —la Comisión de Ciencia y Tecnología (el 1 de febrero de 2016), la Comisión de Inteligencia y Seguridad del Parlamento (el 9 de febrero de 2016) y, sobre todo, la Comisión Mixta del Proyecto de Ley de Potestades de Investigación (el 11 de febrero de 2016)— por su crítica coherente y firme, aunque en ocasiones excesivamente cortés, del proyecto de ley de potestades de investigación, que se tramita actualmente en el Parlamento. La Comisión Mixta del Proyecto de Ley de Potestades de Investigación formuló, en su informe, 86 recomendaciones para que se modificara el proyecto, que versaron sobre las cuestiones de la claridad, la supervisión judicial y la justificación de las diversas potestades. También merece reconocimiento el Gobierno del Reino Unido por haber escuchado los consejos que ha recibido de diversas instancias y por estar aprovechando el proyecto para introducir unos mecanismos muy necesarios de refuerzo de la supervisión. Si bien aún se pueden hacer algunas mejoras en este ámbito, las medidas adoptadas van por buen camino. No obstante, en la fecha de presentación de este informe, el Relator Especial tiene graves dudas acerca del valor de algunas de las modificaciones que se han introducido recientemente en la última versión del proyecto, que se publicó el 1 de marzo de 2016. En la fecha de redacción del presente informe, algunas de las propuestas del Gobierno no solo parecen ir en contra de la argumentación y las conclusiones del informe que presentó en 2014 el Relator Especial sobre la promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, que versaba, entre otras cosas, sobre la vigilancia a gran escala[j], sino que, a primera vista, incumplen los criterios fijados por el Tribunal de Justicia en el caso *Schrems* y los fijados por el Tribunal Europeo de Derechos Humanos en el caso *Zakharov*. El Relator Especial exhorta firmemente a las tres

[i] Véase www.bbc.com/news/world-europe-35007059.

[j] A/69/397.

comisiones a las que acaba de elogiar a que, con vigor y determinación redoblados, sigan ejerciendo su influencia para que las medidas desproporcionadas e invasoras de la privacidad, como la vigilancia y la piratería informática masivas previstas en el proyecto de ley, sean proscritas, y no legalizadas. Parece que el Gobierno no es plenamente consciente de las consecuencias graves y posiblemente imprevistas de legalizar la interceptación y la piratería informática masivas. Teniendo presente la gran influencia que sigue ejerciendo la legislación del Reino Unido en más de la cuarta parte de los Estados Miembros de las Naciones Unidas que siguen formando parte del Commonwealth, así como su honorable tradición como una de las democracias que fundaron los principales órganos regionales de derechos humanos, como el Consejo de Europa, el Relator Especial exhorta al Gobierno a que aproveche esta oportunidad de oro de dar un buen ejemplo y resuelva no adoptar unas medidas desproporcionadas que pueden tener repercusiones negativas mucho más allá de las costas del Reino Unido. Más específicamente, el Relator Especial invita al Gobierno a que muestre mayor empeño en proteger el derecho fundamental a la privacidad de sus propios ciudadanos y los de otros países y también a que desista de dar mal ejemplo a otros Estados al seguir proponiendo medidas, sobre todo la interceptación y la piratería informática masivas, que, a primera vista, contradicen los criterios de varias comisiones parlamentarias del Reino Unido, atentan contra las últimas sentencias del Tribunal de Justicia y el Tribunal Europeo de Derechos Humanos y erosionan el espíritu del propio derecho a la privacidad. Finalmente, el Relator Especial invita al Gobierno a que colabore estrechamente con él, sobre todo en su estudio temático de la vigilancia, a fin de definir unas medidas proporcionadas que potencien la seguridad sin invadir la privacidad en exceso.

6. ¿Los primeros pasos hacia la paz informática?

39. China y los Estados Unidos merecen reconocimiento por haber tomado la iniciativa de empezar a apaciguar la situación en el ciberespacio.

40. Cabe decir que el ciberespacio tiene tres dimensiones principales, todas las cuales se ven amenazadas por el espionaje en línea:

a) El sabotaje y la guerra;

b) Los derechos de propiedad intelectual y el espionaje económico; y

c) Los derechos civiles y la vigilancia.

41. Si bien la privacidad guarda relación, sobre todo, con la tercera dimensión, también suele aparecer en los debates acerca de las otras dos dimensiones. En septiembre de 2015, se anunció que los Estados Unidos y China habían "acordado que ninguno de sus gobiernos apoyaría o practicaría el robo de propiedad intelectual por medios informáticos" y que "ambos países se ha[bía]n comprometido a convenir unas normas apropiadas de comportamiento de los Estados en el ciberespacio dentro de la comunidad internacional. Ambos países también ha[bía]n acordado crear un grupo de especialistas de categoría superior para seguir debatiendo las cuestiones relacionadas con el ciberespacio"[k]. Y los Estados Unidos y China no solo afianzaron ese importante paso hacia delante celebrando unas conversaciones sobre el ciberespacio en diciembre de 2015, sino que también parecen haber sentado un ejemplo para otros países: "al anuncio de los Estados Unidos le siguió un acuerdo análogo entre el Reino Unido y China, y la noticia de que Berlín firmaría un trato 'contra el robo informático' con Beijing en 2016. En noviembre de 2015, China, el Brasil, Rusia, los Estados Unidos y otros miembros del Grupo de los 20 aceptaron la norma que

[k] Véase www.cnbc.com/2015/09/25/us-china-agree-to-not-conduct-cybertheft-of-intellectual-property-white-house.html.

prohibía practicar o apoyar el robo de propiedad intelectual por medios informáticos"[1]. Eso queda aún muy lejos de unos acuerdos completos sobre la guerra informática o la vigilancia en línea y los efectos del espionaje en la privacidad de los ciudadanos, pero al menos es un comienzo, y el Relator Especial no puede sino intentar persuadir a todas las partes interesadas para que amplíen sus conversaciones incluyendo en ellas, asimismo, medidas concretas que garanticen el respeto de la privacidad en línea.

IV. Actividades destacadas del Relator Especial

A. Dotación de recursos para que el Relator Especial ejerza su mandato

42. Dado que el mandato es nuevo, que el presupuesto oficial correspondiente no se aprobó hasta enero de 2016 y que el mandato entró en vigor el 1 de agosto de 2015 —es decir, en una fecha en que la mayor parte de Europa estaba de vacaciones—, el Relator Especial tardó varias semanas en recibir alguna forma de asistencia de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. Por el momento, esa asistencia administrativa es de carácter temporal, hasta que se contrate al personal, contratación que está previsto terminar en junio de 2016 a más tardar. Después de haber examinado la situación en que se hallaba la dotación de recursos, el Relator Especial tomó medidas urgentes para obtener fondos fuera de las Naciones Unidas. Se contrató a un investigador que había terminado su doctorado (un doctorado sobre el tema de la privacidad y el derecho al olvido), en régimen de jornada parcial a partir de octubre de 2015 y en régimen de jornada completa a partir de enero de 2016, para que ayudara en las cuestiones sustantivas. Se mantendrá la financiación externa hasta que se resuelva la situación de la dotación de recursos. Asimismo, han tenido la gran amabilidad de prestar asistencia voluntaria al Relator Especial diversos especialistas y otras personas de instituciones para las que trabaja este, como el Departamento de Políticas y Gobernanza de la Información de la Facultad de Ciencias Mediáticas y del Conocimiento de la Universidad de Malta y el Grupo de Investigación en Seguridad, Tecnología y Privacidad Electrónica de la Facultad de Derecho de la Universidad de Groningen, en los Países Bajos. Esa asistencia, que, junto con la que le presta el personal de las Naciones Unidas en Ginebra, el Relator Especial agradece sobremanera, le permite desempeñar sus funciones hasta que se le dote de capacidad suficiente y disponga de una estructura de apoyo más sostenible y adecuada a sus fines.

B. Una hoja de ruta para el mandato del Relator Especial: formulación del plan de diez puntos

43. Además de a las actividades cotidianas expuestas en la sección II, se ha dedicado un tiempo considerable a elaborar el plan de diez puntos que se enuncia más adelante, en la sección V, y a mantener consultas con los numerosos interesados.

C. Colaboración en numerosas actividades

44. El Relator Especial aceptó invitaciones a reuniones, conferencias y mesas redondas, así como a consultas individuales, sobre todo cuando ayudaban a mantener una política

[1] Véase http://blogs.cfr.org/cyber/2016/01/04/top-5-us-china-cyber-agreement.

continua de colaboración en relación con los siete estudios temáticos ya expuestos. A continuación se ofrece una lista no exhaustiva de tales actividades:

a) Mesa redonda sobre el tema "Unidos indisolublemente: la libertad de expresión y la privacidad en la gobernanza de Internet", MAPPING, Primera Asamblea General, Hannover, Alemania, 22 de septiembre de 2015;

b) Reunión con el Director de Asuntos Mundiales de Human Rights Watch, 30 de septiembre de 2015;

c) Participación y presentación de una ponencia en el Seminario de Protección de Datos y Privacidad en la Estadística, Ginebra, 13 y 14 de octubre de 2015;

d) Reunión con el Secretario General Adjunto de la UIT, Ginebra, 14 de octubre de 2015;

e) Organización y dirección de la mesa redonda sobre privacidad y vigilancia de la Conferencia sobre la Inteligencia en la Sociedad del Conocimiento, Bucarest, 16 de octubre de 2015;

f) Discurso inaugural sobre la privacidad en la era digital en la Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, Ámsterdam, 27 de octubre de 2015;

g) Participación en la mesa redonda "tour du monde" de la Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, Ámsterdam, 29 de octubre de 2015;

h) Participación en numerosas sesiones, públicas y bilaterales, del Foro para la Gobernanza de Internet, João Pessoa, Brasil, 9 a 13 de noviembre de 2015[m];

i) Discurso inaugural en una reunión privada del Seminario Internacional sobre el Tratamiento de Macrodatos en el Sur Global, Río de Janeiro, Brasil, 16 y 17 de noviembre de 2015[n];

j) Reuniones con funcionarios del Ministerio de Justicia del Brasil durante un análisis en profundidad de un nuevo proyecto de ley brasileña de la privacidad, Brasilia, 18 de noviembre de 2015;

k) Reunión conjunta con funcionarios de los Ministerios de Telecomunicaciones, Justicia e Interior del Brasil, para tratar del nuevo proyecto de ley brasileña de la privacidad, Brasilia, 18 de noviembre de 2015;

l) Reunión en la Fiscalía General del Estado, Brasilia, 18 de noviembre de 2015;

m) Reunión con el Director de Derechos Humanos del Ministerio de Relaciones Exteriores del Brasil, Brasilia, 19 de noviembre de 2015;

n) Discurso (por videoconferencia) en el Congreso Mundial de Consumers International, Brasilia, 19 de noviembre de 2015[o];

o) Reuniones y consultas en profundidad con el fundador y director de Patient Privacy Rights, Malta, 25 de noviembre de 2015;

[m] Véase www.intgovforum.org/cms/igf-2015-schedule.

[n] Véase http://itsrio.org/en/2015/11/05/encontro-fechado-workshop-internacional-big-data-no-sul-global.

[o] Véase http://congressprogramme.consumersinternational.org/speakers.html.

p) Discurso durante la sesión introductoria de la Conferencia de Alto Nivel sobre la Protección de la Privacidad en Línea Incrementando la Seguridad de la Tecnología de la Información y la Autonomía de la Unión Europea en materia de Tecnología de la Información, organizada conjuntamente por la Comisión de Libertades Civiles, Justicia y Asuntos de Interior y el Grupo de Evaluación de Opciones Científicas y Tecnológicas del Parlamento Europeo, Bruselas, 8 de diciembre de 2015[p];

q) Discurso inaugural en una conferencia sobre seguridad y privacidad en el ámbito de un puerto seguro 2.0, Roma, 9 de diciembre de 2015[q];

r) Discurso inaugural sobre privacidad, identidad, seguridad y libertad en el congreso anual del Privacy and Identity Lab, Utrecht, Países Bajos, 11 de diciembre de 2015[r];

s) Participación en una sesión de orientación inicial para relatores especiales, Ginebra, 14 a 16 de diciembre de 2015;

t) Reunión con una delegación del Reino Unido, Ginebra, 17 de diciembre de 2015;

u) Reunión con una delegación de China, Ginebra, 17 de diciembre de 2015;

v) Reunión con una delegación de la Federación de Rusia, 17 de diciembre de 2015;

w) Participación, por videoconferencia, en la reunión especial del Comité contra el Terrorismo sobre cómo impedir que los terroristas aprovechen Internet y las redes sociales para reclutar a otros terroristas e instigar atentados, respetando, al mismo tiempo, los derechos humanos y las libertad fundamentales, Nueva York, 17 de diciembre de 2015;

x) Presentación de una ponencia y moderación de los debates en una mesa redonda de ONG en la que participaron representantes de Privacy International, Amnistía Internacional, Reporteros Sin Fronteras, Internet Society, Human Rights Watch y la American Civil Liberties Union, Ginebra, 18 de diciembre de 2015;

y) Reunión con el Director Adjunto de la Oficina de Normalización de la UIT (a la que se unió la Dependencia Jurídica de la UIT), Ginebra, 18 de diciembre de 2015;

z) Intervención y presentación, por videoconferencia, de una ponencia sobre el tema "La privacidad, la calidad de vida y las ciudades inteligentes: la ampliación de 'lo vigilable'", en una conferencia de la UIT sobre las ciudades inteligentes, Singapur, 18 de enero de 2016;

aa) Reuniones con Helen Wallace y Andrew Jackson, de GeneWatch UK, Malta, 3 de febrero de 2016;

bb) Discurso inaugural (por videoconferencia) en el Quinto Seminario sobre la Protección de Datos en las Organizaciones Internacionales, Ginebra, 5 de febrero de 2016[s];

cc) Discurso inaugural y participación en una reunión general de interesados organizada por el Ministerio de Relaciones Exteriores de los Países Bajos, La Haya, Países Bajos, 3 de marzo de 2016.

[p] Véase www.europarl.europa.eu/stoa/cms/cache/offonce/home/events/workshops/privacy.

[q] Véase www.dimt.it/tag/cannataci.

[r] Véase www.pilab.nl/index.php/2015/12/14/the-privacy-identity-lab-four-years-later-published.

[s] Véase www.icrc.org/en/event/5th-workshop-data-protection-within-international-organisations.

V. Plan de diez puntos

45. A fin de desarrollar más pormenorizadamente las dimensiones del derecho a la privacidad y su relación con otros derechos humanos, el Relator Especial ha trazado un plan de acción de diez puntos. Hay que tener presente que los puntos del plan se mencionan en un orden aleatorio que no implica la existencia de un programa de trabajo con una distribución específica de prioridades. El Relator Especial compara su función con la de un explorador. En otros términos, su objetivo es encontrar un camino para avanzar y, al mismo tiempo, determinar las cuestiones urgentes que deben tratarse o reaccionar ante las necesidades urgentes que tengan los particulares o los países en materia de responsabilidad. El plan de acción de diez puntos que se expone a continuación es una lista de cosas que hay que hacer, no una mera lista de deseos. El Relator Especial ya ha empezado a trabajar en cada uno de los diez puntos, pero el progreso vendrá determinado por la disponibilidad de tiempo y recursos.

1. Significado del "derecho a la privacidad"

46. Para trascender el marco jurídico vigente y, así, comprender más profundamente lo que se ha prometido proteger, hay que procurar adquirir una comprensión mejor, más detallada y más universal de lo que se entiende por "derecho a la privacidad". ¿Qué significa y qué debería significar en el siglo XXI? ¿Cómo se lo puede proteger mejor en la era digital? Se organizarán actividades y se apoyarán investigaciones para estudiar posibles respuestas a esas preguntas medulares, que ayudarán a sentar los cimientos esenciales para ejecutar otras partes del plan de acción del Relator Especial.

2. Concienciamiento de la opinión pública

47. Otra cuestión importante es la del concienciamiento de los ciudadanos para ayudarlos a entender lo que es la privacidad. Es importante que haya un discurso general sobre lo que son sus derechos en materia de privacidad y cómo se pueden ver conculcados, sobre todo por las nuevas tecnologías y por el propio comportamiento de los ciudadanos en el ciberespacio. Tienen que aprender cómo se monetizan sus datos personales y cuáles son las salvaguardias y los recursos vigentes que protegen su derecho a la privacidad. ¿Qué pueden hacer para reducir al máximo el riesgo de que se atente contra su derecho a la privacidad y cómo pueden comunicarse con los encargados de formular políticas y con el sector empresarial para mejorar la protección de su privacidad? La labor de concienciamiento es una labor considerable, y el Relator Especial pretende contribuir a ella durante todo su mandato mediante una colaboración constante con todos los interesados, especialmente la sociedad civil.

3. Mantenimiento de un diálogo estructurado y continuo sobre la privacidad

48. Es indispensable entablar un diálogo más estructurado, abierto, amplio, eficaz y, sobre todo, permanente, entre los distintos interesados. Para proteger la privacidad, hay que construir puentes. El Relator Especial pretende dedicar mucho esfuerzo a esa actividad, para lo cual utilizará los foros existentes y creará otros nuevos. A ese respecto es de gran importancia favorecer un diálogo estructurado entre las ONG, las autoridades de protección de datos y privacidad, las fuerzas del orden y los servicios de seguridad e inteligencia. Es esencial colaborar con todas las categorías de interesados para mejorar los procedimientos internos y aumentar el grado de privacidad incorporando medidas para protegerla en el diseño de las tecnologías que se implanten y los procedimientos que se apliquen. Es importante incrementar al máximo la transparencia y la rendición de cuentas y reforzar la supervisón imparcial y eficaz, para que sea mucho más eficaz y digna de crédito.

4. Enfoque integral de las salvaguardias y los recursos legales, procedimentales y operativos

49. Las salvaguardias apropiadas y los recursos jurídicos efectivos han sido parte de la razón de ser del derecho de protección de datos desde el principio. Este derecho aspira a ofrecer unas directrices y una protección apropiadas en un mundo que se ha vuelto cada vez más complejo a causa del cambio tecnológico constante. Habría que brindar una protección más clara y más eficaz a los ciudadanos, a fin de impedir que se invada su privacidad. Hay que ofrecer recursos reales a todos los interesados en caso de que se invada efectivamente su privacidad. La búsqueda de salvaguardias y recursos jurídicos es transversal y subyace a todos los estudios temáticos del Relator Especial, que ya se han enunciado en la sección II.

5. Insistencia redoblada en las salvaguardias técnicas

50. Las salvaguardias y los recursos jurídicos de que disponen los ciudadanos nunca pueden ser puramente legales u operativos. El derecho por sí solo no es suficiente. El Relator Especial seguirá colaborando con el sector técnico para promover la elaboración de salvaguardias técnicas eficaces, como el cifrado, los programas informáticos de superposición y otras soluciones técnicas diversas en las que la privacidad está incluida, de verdad, en el diseño.

6. Diálogo específico con el mundo empresarial

51. Hoy en día, un número cada vez mayor de empresas reúnen ya muchos más datos personales de los que podrán o desearán reunir la mayoría de los Gobiernos. ¿Cuáles son las alternativas admisibles a los modelos de negocio actuales en los que se han monetizado fuertemente los datos personales, o las modificaciones fundamentales que podría prever la sociedad a este respecto? ¿Cuáles son las salvaguardias aplicables en caso de que las autoridades del Estado soliciten datos que se hallen en poder de las empresas? Esta dimensión del mandato requiere mucho tiempo y atención. El Relator Especial ya ha entablado contactos directos con los representantes del mundo empresarial y mantendrá un diálogo sobre esas cuestiones, centrado en la privacidad, con toda una gama de agentes del sector empresarial, a fin de mantenerse informado sobre las novedades que se produzcan en este sector y de facilitarle a este información sobre otras partes de su mandato.

7. Promoción de avances nacionales y regionales en los mecanismos de protección de la privacidad

52. El valor de los avances nacionales y regionales en los mecanismos de protección de la privacidad debería estar más reconocido a nivel mundial. El Relator Especial tiene que desempeñar una importante función complementaria de su labor de cooperación estrecha con las autoridades de protección de datos y privacidad de todo el mundo. Mediante la cooperación recíproca y el diálogo, se podrían elevar sustancialmente los criterios mundiales de protección de la privacidad. El Relator Especial ha empezado a planificar y ejecutar una serie de actividades globales con esas autoridades. Entre ellas se cuentan actividades que está previsto celebrar en Australia, Marruecos, Nueva Zelandia y Túnez, así como en Irlanda del Norte en 2016, y hay muchas otras planificadas para los años venideros.

8. Aprovechamiento de la energía y la influencia de la sociedad civil

53. El Relator Especial, que ya se ha reunido con representantes de 40 ONG durante sus seis primeros meses de mandato, pretende seguir dedicando un tiempo considerable a escuchar a los representantes de la sociedad civil que están haciendo tantos esfuerzos por mejorar la protección de la privacidad en todo el mundo, y a colaborar con ellos.

9. El ciberespacio, la privacidad informática, el espionaje informático, la guerra informática y la paz informática

54. La comunidad mundial tiene que mostrar interés, sinceridad y apertura ante lo que realmente ocurre en el ciberespacio, por ejemplo ante las realidades de la vigilancia a gran escala, el espionaje informático y la guerra informática. La manera de afrontar esas realidades se basará en los resultados de los otros puntos del plan de acción que ya se han expuesto, así como en los resultados de los estudios temáticos mencionados en la sección II. El Relator Especial espera que esas cuestiones figuren, de manera constante, en algunos de sus informes, así como en muchas de sus visitas a países, y, al abordarlas de manera transparente con los interesados, espera desempeñar una labor constructiva de mejora de la protección de la privacidad en la era digital.

10. Aumento de la inversión en el derecho internacional

55. Aunque el derecho por sí solo no sea suficiente, es muy importante. Habría que estudiar, en todas sus formas, la posibilidad de elaborar un derecho internacional sobre la privacidad; el Relator Especial está abierto a examinar el valor de cualquier instrumento jurídico, con independencia de que se lo clasifique como derecho vinculante o derecho no vinculante. Un punto de partida esencial sería ocuparse de una cuestión prioritaria como la de actualizar los instrumentos jurídicos ampliando la comprensión de lo que se entiende por derecho a la privacidad. Parece que hay un consenso entre diversos interesados en el sentido de que uno de esos instrumentos jurídicos podría adoptar la forma de un protocolo adicional del artículo 17 del Pacto Internacional de Derechos Civiles y Políticos[t], y se ha instado al Relator Especial a "promover el inicio de negociaciones sobre dicho protocolo en su primer mandato"[u]. Sin embargo, el calendario preciso de estas negociaciones debería depender probablemente de la duración y el resultado de los debates amplios y profundos sobre el punto 1 ya expuesto, es decir, mejorar la comprensión universal de lo que son, o deberían ser, los valores básicos de la privacidad. Otros asuntos relativos a la privacidad, sobre todo los de la jurisdicción y la territorialidad en el ciberespacio, no se pueden tratar satisfactoriamente si no hay un acuerdo internacional claro a ese respecto; este acuerdo debería adoptar normalmente la forma de un tratado multilateral que versara, con toda probabilidad, sobre un tema concreto o un conjunto de temas. Así pues y para despejar las dudas, cabe afirmar que lo que se prevé no es una convención internacional nueva, global y universal, que abarque todas las cuestiones relativas a la privacidad o la gobernanza de Internet. Es mucho más realista suponer que la protección de la privacidad se pueda potenciar mediante el desarrollo gradual del derecho internacional y, por tanto, mediante la clarificación y, en último término, la ampliación de los instrumentos jurídicos vigentes. Ello significa que, a medio y a largo plazo, se podrían elaborar instrumentos jurídicos completamente nuevos. El Relator Especial también prestará atención a los debates actuales sobre el derecho internacional y los nuevos instrumentos jurídicos en el ámbito de la gobernanza de Internet, a fin de determinar el calendario de actividades de los órganos de las Naciones Unidas, y el tipo y el ámbito de aplicación del instrumento jurídico que el Relator Especial pueda, en última instancia, desear recomendar al Consejo de Derechos Humanos y a la Asamblea General.

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

[u] *Ibid*.

VI. Conclusiones

56. **Al Relator Especial le ha impresionado la acogida extremadamente calurosa y entusiasta que ha recibido de la mayoría de los sectores de la sociedad y la mayoría de las diversas categorías de interesados.**

57. **La privacidad no ha ocupado nunca un lugar tan importante en la conciencia política, judicial o personal como en 2016.**

58. **Las tensiones entre seguridad, modelos de negocio de las empresas y privacidad siguen ocupando el centro del escenario, pero en los últimos 12 meses se han registrado indicios contradictorios: algunos Gobiernos han seguido, en la práctica o en el Parlamento, adoptando actitudes hostiles hacia la privacidad, mientras que los tribunales de todo el mundo, especialmente los de los Estados Unidos y Europa, han lanzado apuestas firmes a favor del derecho a la privacidad y sobre todo en contra de las medidas desproporcionadas e invasoras de la privacidad, como la vigilancia a gran escala o el descifrado.**

59. **Hay indicios sólidos de que la privacidad se ha convertido en una consideración comercial importante, ya que algunas empresas de gran envergadura la han adoptado como gancho comercial. Si hay un mercado para la privacidad, las fuerzas del mercado lo desarrollarán. El veloz incremento de la disponibilidad de dispositivos y servicios de programación informática con cifrado es un indicio sólido de que los consumidores de todo el mundo son cada vez más conscientes de los riesgos que acechan a su privacidad y de que preferirán, cada vez más, los productos y los servicios que protejan su privacidad a los que sean neutrales a ese respecto o atenten contra ella.**

60. **Aunque algunos Gobiernos prosigan con sus intentos insensatos, desacertados, imprudentes, inoportunos y, en ocasiones, irrespetuosos de legalizar o aplicar unas medidas desproporcionadas e injustificables que atentan contra la privacidad, como la recopilación masiva de datos, la piratería informática masiva y la interceptación sin garantías jurídicas, otros Gobiernos, encabezados en este caso por los Países Bajos y los Estados Unidos, se han decantado más abiertamente por una política de prohibición de las puertas traseras para acceder a la información cifrada. El Relator Especial desearía exhortar a más Gobiernos a que se sumaran a esta segunda postura.**

61. **Los países de todo el mundo no solo están empezando a reconocer sus responsabilidades y la realidad de la existencia de salvaguardias técnicas como el cifrado, sino que también se están dando cuenta, lenta pero inexorablemente, de los beneficios escasos que les reportaría destruir el ciberespacio mediante la guerra y el espionaje informáticos y los gravísimos riesgos que ello entrañaría. Hay que progresar más en esta esfera, pero en 2015 se dieron algunos primeros pasos importantes. Por tanto, el Relator Especial exhorta a los Gobiernos, y no solo a los del Grupo de los 20, a que se reúnan en torno a una mesa para debatir cuál debe ser el comportamiento apropiado de los Estados en el ciberespacio y qué medidas de gobernanza se deben adoptar a ese respecto, tomando en consideración, entre otras cosas, los derechos civiles, y sobre todo la privacidad, la libertad de expresión y la vigilancia.**

62. **Los métodos de trabajo del Relator Especial y el plan de diez puntos deberían dar testimonio de la aplicación de un enfoque holístico al tema de la protección y la promoción de la privacidad en la era digital. Un enfoque holístico ayuda a determinar el cuadro general de lo se deba hacer, si bien el cálculo de lo que se deba hacer exactamente, quién lo deba hacer y cuándo dependerá de dos factores principales: en primer lugar, los recursos disponibles para aplicar el plan de acción y terminar los estudios temáticos y, en segundo lugar, la voluntad de los diversos interesados de**

aceptar y promover un programa de defensa de la privacidad, en lugar de aferrarse a "una mentalidad de mando y control". El mensaje del Relator Especial para los que, a primera vista, estimen que el plan de acción no es ya ambicioso sino quizá demasiado ambicioso es claro y sencillo: si están ustedes de acuerdo con los objetivos del plan y con la integración que se hace en él de una serie de cuestiones complejas pero interrelacionadas, entonces den un paso al frente y aporten recursos adicionales para aplicarlo. Ello ayudará a incrementar su viabilidad. El Relator Especial aprovecha su experiencia como administrador de proyectos con un historial profesional exitoso, a lo largo del cual ha recaudado decenas de millones dólares destinados a investigaciones privadas, para trazar una estrategia que le permita incrementar los recursos de que dispone como titular de un mandato; en realidad, el plan de diez puntos se ha elaborado apostando por el éxito de esa estrategia. Aun cuando esa estrategia sea un éxito total, el Relator Especial está firmemente convencido de que la continuación y la (posible) terminación de algunas partes del plan de diez puntos recaerán en el próximo titular del mandato. Lo que hay que hacer en esta etapa es ofrecer una visión clara y completa y sentar unos cimientos firmes que sirvan de base a una política sólida y empírica de protección de la privacidad.

Annex I

Challenges faced by the Special Rapporteur and his vision for the mandate

1. The Special Rapporteur immediately set about building up his team composed of persons working for the mandate on a part-time or full-time basis. One of these persons is currently a full-time United Nations (UN) Human rights officer, hired on a temporary contract, while the position is under recruitment. The work of this person is supervised by a more senior UN employee who is also responsible for supporting the work of six other mandate holders. A second part time professional and a part time administrative officer will soon be recruited, as well as a part-time consultant. The SRP is grateful that the Human Rights Council endowed his mandate with this still limited (given the scope of his mandate) but unprecedented level of support to a mandate holder. The other persons in the SRP team are not employed by the UN but are resourced by extra-mural funding obtained by the SRP or may be volunteers. The team is often physically spread across at least three geographical locations (currently Malta, the Netherlands and Switzerland) and, as befits the digital age, most of the team meetings are carried out in cyber-space with the working day being opened by an on-line conference call involving all team-members who may be available. During the "morning meeting" team members typically report on work carried out in the previous day, consult about tasks planned for the rest of the working day and plan tasks and events for the following weeks and months. When doing so, their tasks reflect the fact that the work of the SRP may be broadly divided into four categories and any team member may be working concurrently on tasks from each of these categories.

2. The fact that the mandate on privacy is a new one presents both advantages and disadvantages. Amongst other things it means that the Special Rapporteur on Privacy (SRP) had no roadmap to follow and indeed one of his first priorities in this case is to work on designing and developing such a roadmap. This means that some of the issues identified in this and later reports are not necessarily capable of being resolved within the time-constraints imposed by one or even two three-year mandates. They are mentioned however in order to provide a more holistic picture of what needs to be done in the short, mid and long-term. In doing so, this incumbent is conscious of possibly identifying issues which may possibly be more appropriately tackled in a more timely manner by later holders of the mandate.

3. One of the recurring themes of this and later reports will undoubtedly be the time dimension. The rapid pace of technology and its effects on privacy means that action on some already-identified issues may increase or decrease in priority as time goes by while new issues may emerge fairly suddenly. It may also mean that sometimes it may be more opportune to launch or intensify action on a particular issue not necessarily because it is much more important than other issues but rather because the timing is right, because the different international audiences and classes of stakeholders may be far more sensitive and receptive to that particular issue for reasons and circumstances over which the Special Rapporteur may have absolutely no control but in which case it would be foolish not to take advantage of favourable opportunities which may result in the creation or improvement of privacy safeguards and remedies.

4. The later prioritisation of action will also depend on the extent of the resources made available to the Special Rapporteur and the extent to which he can succeed in attracting fresh resources to support the mandate on privacy. This resource issue is fundamentally important and will directly affect the extent of the impact the mandate on Privacy may have

in practice in real life. It is clear that, however good in quality in some respects, the quantity of resources provided to the mandate by the UN is woefully inadequate and even if the mandate's human and financial resources are increased tenfold, it would still be hard-pressed to achieve the minimum required to persuade the incumbent that the work of the mandate is really making a difference to the protection of privacy of ordinary citizens around the world. The experience of the first six months in office has persuaded the mandate-holder that not only must the SRP be omni-present 24/7 on the many privacy-related issues which arise literally every day in many countries around the world but that he must also act as rainmaker, somehow attracting funds and human resources in order to make the work of the mandate both possible and sustainable in the short, mid and long-term. The effort required by what is, in essence, a part-time, un-paid position which must, by definition, co-exist with a demanding day-job, should not be under-estimated. This effort can be encouraged by the positive response of all stakeholders not least that of the nation-states, members of the UN to whom this report is addressed. If these stakeholders do not support the mandate adequately, if they do not put their money where their mouth is, then this will only serve to increase the frustrations already inherent to any work being carried out within the UN's systems and bureaucracy.

5. The incumbent's vision of the mandate is therefore analogous to the process required to design, finance, project manage and complete the building of a house or other building suitable for human beings to live and/or work in safely. Firstly we need to understand the function of the building: is it a residence for an individual living alone or for one nuclear family, or for a large and extended family or indeed for several of such individuals and families? Should it include a working space and if so for what type of work: is this to be a farm-house, a baker's *casa bottega* or a black-smith's lodge or an urban block of multi-rise apartments? Form follows function so the function or functions must be clearly identified and understood in-depth. Secondly, form follows function so the design of the house — or the mandate's range of activities — must be completed on the basis of the function. Thirdly, the size of the building and its interior may be basic, cramped, spartan i.e. just barely enough to provide basic shelter and sanitation or else it may be more comfortable and spacious and functional or else it may be downright luxurious. Whether it is one or the other will depend on the resources and especially the finances which can be projected to be available to the builder — and these will influence the final design of the plan for the building — and the mandate. Fourthly, the time available to complete essential parts of the building will also influence the design of the plan. Fifth, it will need to be borne in mind that life gets in the way of the best-laid plans and the design may, from time to time, have to be more of an emergent design process rather than the fulfilment of a rigid, prescriptive pre-ordinate design. This analogy is useful to explaining the scope of this report especially to emphasize that while the building itself may not necessarily be capable of completion within the time-frame of one or even two three-year mandates, it is very important to decide on what the final building needs to be like, otherwise we would be unable to design the type of the foundations we require to build...and unless the foundations are sound and fit-for-purpose the building will ultimately prove to be unsustainable and collapse.

Annex II

A more in-depth look at open data and big data

1. One of the most important issues in information policy and governance in the second decade of the twenty-first century deals with determining the *medio stat virtus* between, on the one hand, use of data for the benefit of society under the principles of Open Data and, on the other hand, the established principles we have developed to date with a view to protecting fundamental rights like privacy, autonomy and the free development of one's personality.

2. At first sight Open Data sounds fine as a concept, a noble and altruistic approach to dealing with data as a common good, if not quite "common heritage of mankind". Who could object to data sets being used and re-used in order to benefit various parts of society and eventually hopefully all of humanity? It is what you can do with Open Data that is of concern, especially when you deploy the power of Big Data analytical methods on the data sets which may have been made publicly available thanks to Open Data policies. Of course, it is important to differentiate between data sets of one type and another. If what is put into the public domain consists of, say, the raw data arising out of tens of thousands of questionnaire responses about perceptions of privacy which responses would have been gleaned from across 27 EU member states and processed in an anonymised manner, the risk to individual privacy from aggregated data sets would appear to be very low if not non-existent. If, on the other hand, one uses Big Data analytical methods to develop links between supposedly anonymized medical data and publicly available electoral registers in a way that links identified or identifiable individuals to sensitive patient information then society has genuine cause for concern. Pioneers like Latanya Sweeney in the USA have demonstrated these abilities and exposed these risks on numerous occasions over the past two decades but the question remains: how should society intervene? More precisely how should policy-makers act in the face of such risks? Which is the correct information policy to develop and adopt? Especially since society has already intervened in a number of ways. Open Data is an information policy born out of specific information politics. For example, the EU legislated in favour of re-utilising public data more than 12 years ago (Directive 2003/98/EC), indeed five years after Prof Sweeney's first eye-opening discoveries.[a] Is this one of many cases where Open Data Policies were embraced before unintended consequences were properly understood and may now need to be remedied?

3. It is sometimes not widely appreciated how fundamental a challenge Open Data represents to the most important principles in data protection and privacy law world-wide. For the best part of forty years, our entire *forma mentis* has been founded upon something

[a] "In 2000, Sweeney analyzed data from the 1990 census and revealed that, surprisingly, 87 percent of the U.S. population could be identified by just a ZIP code, date of birth, and gender" according to Caroline Perry, SEAS Communications "You're not so anonymous" October 18, 2011 last accessed on 13 Jan 2016 at http://news.harvard.edu/gazette/story/2011/10/you%E2%80%99re-not-so-anonymous/ . However, in testimony to the Privacy and Integrity Advisory Committee of the Department of Homeland Security ("DHS") on 15 June 2005 Sweeney states that it was in 1997 that she "was able to show how the medical record of William Weld, the governor of Massachusetts of the time could be re-identified using only his date of birth, gender and ZIP. In fact, 87% of the population of the United States is uniquely identified by date of birth (e.g., month, day and year), gender, and their 5-digit ZIP codes. The point is that data that may look anonymous is not necessarily anonymous". http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_06-2005_testimony_sweeney.pdf last accessed on 13 January 2016.

we call the purpose-specification principle. Put simply, personal data should be collected, used, stored and re-used for a specified legitimate purpose or for a compatible purpose. Once the time required for the data to be stored by that specified purpose runs out then the data should be deleted permanently. Re-using personal data is not part of our privacy or data protection DNA.

4. The purpose-specification principle is not something invented by Europeans. One of the first places where it is articulated as such is in a 1973 report by an Advisory Committee to the US Department of Health[b] where it was held that "There must be a way for an individual to prevent personal information used for one purpose from being used or made available for other purposes without his or her consent". This quickly became a fundamental value in many other fora. The OECD Guidelines of 1980 have the Purpose specification Principle as the third out of eight principles "The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose". In this context it is also important to note the OECD's corollary fourth principle usually recognised as the Use Limitation Principle whereby "Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with 3 above except a) with the consent of the data subject; or b) by the authority of law" These principles are also found in the Council of Europe's influential Data Protection Convention of 1981 and the EU's Data Protection Directive (46/95).

5. In an important regional development, the European Union is now at an advanced stage of devising and implementing the next generation of its data protection laws. When one examines the texts produced by the EU between 2012 and 2015, it is not as if the European Union appears ready to abandon the principle of purpose limitation. In the latest available version[c] of the draft text of the EU's General Data Protection Regulation (GDPR) the importance of the purpose specification principle does not appear to be in any way to be diminished. Article 5 b retains the principle prominently, stipulating that personal data shall be

> (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;

an approach reinforced by the next principle to be found in the GDPR's Article 5 which lays down that personal data shall be

> (c) adequate, relevant, and limited to the minimum necessary in relation to the purposes for which they are processed; they shall only be processed if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data;

[b] DHEW Secretary's Advisory Committee on Automated Personal Data Systems, *Records, Computers and the Rights of Citizens*, U S Govt. Printing Office, Washington USA 1973 at p. 41.

[c] s_2014_2019_plmrep_AUTRES_INSTITUTIONS_COMM_COM_2015_12-17_COM_COM(2012)0011_EN.pdf.

6. The meaning of these key principles had been similarly announced in the recitals of the GDPR

> (30) Any processing of personal data should be lawful, fair and transparent in relation to the individuals concerned. In particular, the specific purposes for which the data are processed should be explicit and legitimate and determined at the time of the collection of the data. The data should be adequate, relevant and limited to the minimum necessary for the purposes for which the data are processed; this requires in particular ensuring that the data collected are not excessive and that the period for which the data are stored is limited to a strict minimum. Personal data should only be processed if the purpose of the processing could not be fulfilled by other means. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. In order to ensure that the data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review.

7. It is clear therefore that the current thinking in Europe on Data Protection still relies on the purpose specification principle taken in tandem with anonymization or deletion despite all the risks inherent in the use of Big Data Analytics and Open Data. Likewise, in the United States where on May 9, 2013, President Obama signed an executive order[d] that made open and machine-readable data the new default for government information",[e] some have attempted to downplay the concerns raised by Latanya Sweeney and have generally held that the risks of de-identification are not as great as previously made out.[f] Yet, a detailed analysis of the output of Prof Sweeney's Data Privacy Lab[g] and some of her more recent research[h] persuade the SRP that we are running the risk of using outmoded safeguards, almost twenty years after our attention was drawn to the fact that stripping personal data of some basic identifiers may not be enough to protect privacy.

8. A careful examination of the pivotal thinking in Europe in 2015-2016 does not provide much reassurance especially if one carefully examines the pertinent part of the latest version[i] available of the draft EU General Data Protection Regulation which holds that

> (23) The principles of protection should apply to any information concerning an identified or identifiable person. To determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the individual. The principles of data protection should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable.

[d] https://www.whitehouse.gov/the-press-office/2013/05/09/executive-order-making-open-and-machine-readable-new-default-government- last accessed on 13 Jan 2016.

[e] https://www.whitehouse.gov/open last accessed on 13 January 2016.

[f] See for example Barth-Jones, Daniel C. "The "Re-identification" of Governor William Weld's Medical Information: A Critical Re-examination of Health Data Identification Risks and Privacy Protections, Then and Now" June 2012 last accessed on 13th January at https://fpf.org/wp-content/uploads/The-Re-identification-of-Governor-Welds-Medical-Information-Daniel-Barth-Jones.pdf.

[g] http://dataprivacylab.org/index.html.

[h] Sweeney L, Matching Known Patients to Health Records in Washington State Data, 2012 last accessed on 13th January 2016 at http://dataprivacylab.org/projects/wa/1089-1.pdf.

[i] http://www.emeeting.europarl.europa.eu/committees/agenda/201512/LIBE/LIBE%282015%291217_1/sitt-1739884 last accessed on 13th January 2016.

9. This latest version from December 2015 after negotiation with the Council is less detailed than the one approved by the Parliament in October 2013 which held that

> (23) The principles of data protection should apply to any information concerning an identified or identifiable natural person. To determine whether a person is identifiable, account should be taken of all the means reasonably likely to be used either by the controller or by any other person to identify or single out the individual directly or indirectly. To ascertain whether means are reasonable likely to be used to identify the individual, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration both available technology at the time of the processing and technological development. The principles of data protection should therefore not apply to anonymous data, which is information that does not relate to an identified or identifiable natural person. This Regulation does therefore not concern the processing of such anonymous data, including for statistical and research purposes.

10. Is the change an improvement, a factor which strengthens privacy protection in the era of Open Data or Big Data or is it a compromise which weakens protection? Whereas, it seems to the SRP that the very standard formulation of October 2013,[j] dependant as it was on the costs and time required to identify an individual, is rapidly becoming archaic in the era of big data analytics, the rather vaguer 2015 version seems to be a bit more elastic, but that could be a double-edged sword. If we are to insist on maintaining information policies built around the principles of Open Data then we need to develop much stronger, complex algorithmic solutions and procedural safeguards. The application of the newest EU proposals pivot almost entirely on what constitutes anonymous data yet Latanya Sweeney[k] and others have clearly demonstrated that there are huge limits to anonymization and it would seem that practically most personal data may actually be identifiable with such minimal effort that they would not meet eligibility criteria to qualify as anonymous data, thus bringing the GDPR into play.

11. Things get even more complicated when taking into consideration the factors legitimising research[l]

> (88) For the purposes of processing for historical, statistical and scientific research purposes, the legitimate expectations of society for an increase of knowledge should be taken into consideration.

12. While the issue of sensitive data such as health information still presents a quandary within the EU's GDPR

> (42) Derogating from the prohibition on processing sensitive categories of data should also be allowed if done by a law, and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where grounds of public interest so justify and in particular for health purposes, including public health and social protection and the management of health-care services, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system, or for historical, statistical and scientific research purposes.

[j] "inofficial consolidated version" https://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf last accessed on 13th January 2016.

[k] http://latanyasweeney.org/publications.html.

[l] Though this recital 88 has been expanded in the latest 17 Dec 2015 version.

13. How do Open Data and Big Data analytical capabilities fit into the scenarios and thinking portrayed above? Which would be the suitable safeguards to apply in Open Data policies which would protect privacy in the era of Big Data? Are the latest legal innovations being contemplated in Europe the right response to the evidence presented by Sweeney and do they represent best practice for the world to follow or dubious practice for the world to shun? The only thing that is certain is that if we are to get things right then it is clear that we need much more in-depth analysis of both the risks of Open Data as well as existing and new safeguards. Moreover, in this field too there appears to be a huge need for increasing public awareness. Relatively few people seem to know about the existence of open data policies or the consequences of applying big data analytics to different data sets put into the public domain by Open Data policies. In the course of participating in debates about Open data and Big data during tenure as SRP, one reinforced the impression that Open Data policies and their privacy and autonomy implications remain very much an area of interest to a tiny group of domain specialists and then again may be restricted further by the language in which they are made available to the public. The SRP is very sensitive to and is working with NGOs interested in protecting personal data in a number of sectors, including medical data and will, during 2016-2017 be engaging in events aimed at promoting discussion and on-going, in-depth investigation of related matters. The SRP is also very concerned that entire nations or trading blocs including major nations or regional federations such as China, the European Union and the United States have adopted or are adopting Open Data and Big Data policies the far-reaching consequences of which may not as yet be properly understood and which may unintentionally put in peril long-standing social values as well as the fundamental rights to privacy, dignity and free development of one's personality. Some studies on posthumous privacy suggest that in 2016 the citizens of some countries may be better off dead from a privacy point of view since their rights to privacy are better protected by law if they are dead than if they are alive in a world where Open data and big data analytics are a way of life endorsed by the information policies of the countries concerned. These developments may well be unintentional but the impact on privacy, autonomy, dignity and free development of personality may be far-reaching.

Annex III

Further reflections on the notion of privacy

A. Core values and cultural differences

1. As a result of the processes described in Section III of the report, an improved, more detailed understanding of privacy should be developed by the international community. This understanding should possibly result in some flexibility when it comes to addressing cultural differences at the outer fringes of the right or in privacy-neighbouring rights while clearly identifying a solid and universally valid core of what privacy means in the digital age.

2. This global concept of privacy has to pass the test of being positively describable and definable as a precious substantive right on the one hand. On the other hand there also needs to be a negative understanding of the right which hints at legitimate limitations should it be legitimate and necessary to restrict privacy in a proportionate manner. The Special Rapporteur invites all actors in the field to contribute to the development of this urgently needed and improved understanding of the right to privacy and is convinced that significant progress is possible.

B. Enforcement

3. Apart from the absence of a clear universal understanding of privacy, the lack of effective enforcement of the right is an issue which is evident at most turns of the debate. Thus, not only is it not entirely clear what needs to be protected but also how to do it. Regretfully though perhaps hitherto inevitably, the super-fast development of privacy-relevant technologies and especially the Internet has led to a huge organic growth in the way in which personal data is generated and the exponential growth in the quantity of such data. This is especially evident in an on-line environment where, when seen from a global perspective, it would appear that the triangle of actors consisting of legislators, private (mostly corporate) actors and citizens all try to shape cyberspace using their possibilities in an uncoordinated manner. This may lead to a situation where none of the three is able to unleash the full potential of modern information technology.

4. In order to disentangle this triangular relationship an ongoing and open dialogue needs to be set up which eventually would provide for a more clear and harmonious regulation of cyberspace. This can only be achieved as a result of a sincere, open and committed dialogue of all parties which is to be held in a respectful and open manner. Sturdy and reliable bridges need to be built between all actors which are shaping the developments. It is the intention of the Special Rapporteur to listen closely to all parties and to facilitate this dialogue. In this way a basis for a positive and sustainable long-term development in the field of privacy protection should be achieved.

Annex IV

A "State of the Union" approach to privacy

It would appear to be useful to, at least once a year, have the SRP present an independent stocktaking report on where the right to privacy stands and this may be one of the primary functions of both the reports to be made to the Human Rights Council (HRC) and the General Assembly (GA). Since these reports are constrained by a word-limit it is clear that they can be little more than an extended executive summary of the findings and activities of the mandate throughout the reporting period. It should follow that the reports will also reflect the working methods of the mandate as outlined in Section II of the main report, in particular the thematic investigations as well as salient developments identified in the country monitoring activities carried out by the SRP team. It is expected that the report presented to the March 2017 session of the Human Rights Council would be the first such report reflecting a "State of the Union" approach. The report to the March 2016 session of the HRC will not attempt to prioritise risks or landmark improvements in privacy protection but simply refer to a few cases which illustrate particular progress or difficulties.