Asamblea General

Distr. general
6 de septiembre de 2017
Español
Original: inglés

Consejo de Derechos Humanos
34º período de sesiones
27 de febrero a 24 de marzo de 2017
Tema 3 de la agenda
Promoción y protección de todos los derechos humanos, civiles, políticos, económicos, sociales y culturales, incluido el derecho al desarrollo

Informe del Relator Especial sobre el derecho a la privacidad*

Nota de la Secretaría

En su informe, elaborado en cumplimiento de la resolución 28/16 del Consejo de Derechos Humanos, el Relator Especial sobre el derecho a la privacidad se centra en las actividades de vigilancia de los organismos del Estado desde una perspectiva nacional e internacional. El Relator Especial expone en detalle las características del marco jurídico internacional y ofrece una interpretación de dicho marco. También describe los últimos acontecimientos y tendencias, la forma en que pueden estudiarse y el modo en que interactúan con el disfrute del derecho a la privacidad y otros derechos humanos interrelacionados. Consiguientemente, presenta enfoques preliminares para supervisar de una manera más favorable a la privacidad las actividades de vigilancia realizadas por los organismos del Estado. Por último, el Relator Especial informa sobre sus actividades en el período abarcado por el informe.

* El presente documento se presentó con retraso para incluir información lo más actualizada posible.

Informe del Relator Especial sobre el derecho a la privacidad

Índice

I. Introducción

1. Conforme a lo dispuesto en la resolución 28/16 del Consejo de Derechos Humanos, el Relator Especial sobre el derecho a la privacidad presenta informes anuales al Consejo y a la Asamblea General. Este es el segundo informe que presenta al Consejo. En el informe anterior, el Relator Especial expuso un plan de acción de diez puntos y una estrategia para abordar algunas cuestiones contemporáneas decisivas relacionadas con su mandato mediante actividades en "líneas de acción temáticas". El Relator Especial espera que estas iniciativas contribuyan a aumentar el grado de respeto, protección y cumplimiento del derecho a la vida privada, amenazada en particular por los cambios producidos en la era digital.

2. El Relator Especial publicó recientemente una declaración sobre la planificación de los informes temáticos y la solicitud de colaboraciones, en la que presentó las cuestiones que se iban a abordar en este informe y en informes futuros y estableció un calendario para la presentación de sus informes[1]. La declaración debe considerarse como una invitación abierta a los interesados de todos los países del mundo que quieran colaborar con el mandato. Toda persona que desee contribuir o participar de alguna otra manera en cualquiera de las iniciativas mencionadas deberá ponerse en contacto con el Relator Especial o los miembros de su equipo, de preferencia por correo electrónico (srprivacy@ohchr.org), y el Relator Especial o su equipo responderán lo antes posible.

3. Como se indica en el resumen, el presente informe del Relator Especial se centra en los enfoques preliminares para supervisar de una manera más favorable a la privacidad las actividades de vigilancia de los organismos del Estado. El Relator Especial ya ha realizado varias actividades sobre este tema durante su mandato y continuará haciéndolo. Con el fin de cumplir con las tareas descritas en su informe anterior (A/HRC/31/64), particularmente en el sector de la vigilancia, el Relator Especial invirtió esfuerzos considerables en la organización del Foro Internacional de Supervisión de los Servicios de Inteligencia, celebrado en Bucarest los días 11 y 12 de octubre de 2016, y organizado conjuntamente por la Comisión Conjunta de la Cámara de Diputados y el Senado para el control parlamentario de las actividades del Servicio de Inteligencia de Rumania, la Comisión Especial de la Cámara de Diputados y el Senado para el control parlamentario de las actividades del Servicio de Inteligencia Exterior, y las Comisiones de Defensa, Orden Público y Seguridad Nacional de la Cámara de Diputados y el Senado, en colaboración con el Departamento de Políticas y Gobernanza de la Información de la Universidad de Malta y el Grupo de Investigación en Seguridad, Tecnología y Privacidad Electrónica de la Universidad de Groningen, de los Países Bajos. La reunión fue muy positiva, teniendo en cuenta sus comprensiblemente modestos objetivos[2]. Por consiguiente, el Relator Especial tiene la intención de seguir participando en la organización anual del Foro. Está previsto que el Foro de 2017 se celebre los días 20 y 21 de noviembre en Bruselas, y será organizado, entre otras entidades, por la Comisión de Protección de la Vida Privada, que es el organismo encargado de la protección de datos de Bélgica. Se prevé que el Foro permitirá que el Relator Especial desempeñe su mandato aprovechando la experiencia práctica y los conocimientos operacionales adquiridos por los numerosos órganos de supervisión que se han establecido en todo el mundo. Esto le permitirá comprender y analizar mejor las realidades de las iniciativas destinadas a lograr una supervisión efectiva de las actividades de los servicios de seguridad y de inteligencia, así como las consecuencias que ello pueda tener en la privacidad. El primer Foro reunió a casi 70 participantes de unas 26 instituciones

[1] La declaración puede consultarse en www.ohchr.org/EN/Issues/Privacy/SR/Pages/ThematicReports.aspx and www.privacyandpersonality.org/2016/12/united-nations-mandate-of-the-special-rapporteur-on-the-right-to-privacy-planned-thematic-reports-and-call-for-consultations/.

[2] Los objetivos del Foro, tal como se indicó en la invitación formal remitida a los Estados, eran: entablar un debate abierto y franco en un marco de confianza sobre la idoneidad de los mecanismos de supervisión; las medidas de vigilancia existentes y previstas que pudieran tener consecuencias negativas para la privacidad; la distinción entre vigilancia específica y vigilancia a gran escala; la proporcionalidad de tales medidas en una sociedad democrática; y la eficacia en función de los costos y general de esas medidas.

procedentes de 20 países, entre los que había organismos independientes de supervisión, comisiones parlamentarias, algunos miembros de la sociedad civil e incluso un tribunal de supervisión. El Relator Especial considera que una mejor concepción y dotación de recursos de la supervisión de las actividades de inteligencia es una de las muchas iniciativas complementarias que pueden contribuir a mejorar la protección del derecho a la privacidad en todo el mundo. Hay quienes consideran que esta es la vía más adecuada para conseguir medidas concretas que protejan la vida privada. Sin embargo, eso es algo que todavía no se ha demostrado. Cabe esperar que esta serie de foros anuales contribuya a la identificación y el intercambio de buenas prácticas y que, en última instancia, refuerce considerablemente los mecanismos de supervisión en numerosos Estados Miembros. También cabe esperar que los mecanismos de supervisión estén firmemente fundamentados en leyes nacionales precisas y estrictas que prevean únicamente las medidas proporcionales necesarias en una sociedad democrática y que dispongan salvaguardias adecuadas. La legislación también debe consolidar una supervisión efectiva tanto de las fuerzas del orden como de los servicios de seguridad e inteligencia a través de órganos de supervisión independientes y dotados de recursos suficientes. Sobre la base de los debates en los Foros anuales, el Relator Especial espera formular recomendaciones para velar por la promoción y la protección del derecho a la privacidad, en particular respecto de los retos que plantean las nuevas tecnologías, en cumplimiento de su mandato.

4. En relación con la vigilancia, el Relator Especial no se ha centrado solamente en los mecanismos de supervisión, sino que también ha prestado especial atención y hecho un seguimiento, en la medida de lo posible a nivel mundial, de los nuevos informes y proyectos de ley pertinentes sobre el uso o el abuso de la vigilancia. Como consecuencia, la actividad relacionada con la vigilancia es una de sus principales consideraciones cuando solicita visitas oficiales a los países. Esto puede verse especialmente en la elección de las próximas visitas a países: Estados Unidos de América (del 19 al 24 de junio de 2017), Francia (visita solicitada del 13 al 17 de noviembre de 2017), Reino Unido de Gran Bretaña e Irlanda del Norte (visita solicitada para finales de 2017, posiblemente del 11 al 17 de diciembre), Alemania (visita solicitada del 29 de enero al 2 de febrero de 2018) y República de Corea (visita solicitada del 3 al 15 de julio de 2018). Se trata de Estados con sólidas tradiciones democráticas y el Relator Especial espera que asuman un papel de liderazgo en la definición de las mejores prácticas y las salvaguardias en el ámbito de la vigilancia y los derechos humanos fundamentales, especialmente el derecho a la privacidad. Además, estos países han tenido una participación especialmente activa en el ámbito de la vigilancia durante los últimos años, tanto en lo que respecta a la aplicación de tecnologías de vigilancia como a la adopción de nueva legislación. Para cada visita, el Relator Especial ha solicitado reuniones con las autoridades de los servicios de inteligencia y los organismos de supervisión, así como con los ministros responsables de las fuerzas del orden y los servicios de seguridad y de inteligencia.

5. Además, para evitar reinventar la rueda y con el objetivo de maximizar las sinergias, el titular del mandato sigue muy de cerca los procesos y los resultados de otras iniciativas paralelas, como el proyecto sobre alternativas de gestión en materia de privacidad, propiedad intelectual y gobernanza de internet (proyecto MAPPING), apoyado por la Unión Europea, que tiene por objeto promover un entendimiento integral y "conjunto" de los numerosos y diversos aspectos económicos, sociales, jurídicos y éticos de la reciente evolución en Internet y sus consecuencias para las personas y la sociedad en general. El proyecto MAPPING, que se puso en marcha en 2014, más de un año antes de que el Consejo de Derechos Humanos estableciera el mandato del Relator Especial y 18 meses antes de que este asumiera su cargo, ha iniciado varios debates relativamente bien dotados de recursos entre las partes interesadas, entre ellos uno sobre la creación de un instrumento jurídico internacional para regular las actividades de vigilancia. Está previsto que esos debates continúen hasta finales de febrero de 2018. El Relator Especial tiene la intención de seguir los resultados de esos debates y pronunciarse sobre la conveniencia y la viabilidad de dicho instrumento jurídico internacional entre marzo y julio de 2018. Es posible que exponga su postura en el informe que presentará a la Asamblea General en octubre de 2018 y que probablemente formule recomendaciones al respecto para velar por la promoción y la protección de la privacidad, por ejemplo respecto de los retos que plantean las nuevas tecnologías, específicamente en cumplimiento de su mandato.

6. El Relator Especial también mantiene contacto y colabora con otras personas o entidades que están emprendiendo iniciativas destinadas a establecer un marco coherente para la supervisión internacionalmente coordinada de las actividades de inteligencia. En los últimos 18 meses de intensa labor el Relator Especial ha establecido o afianzado muchas provechosas relaciones de trabajo en todo el mundo con autoridades interesadas en trabajar en algún tipo de instrumento que establezca normas comunes para la realización de las funciones de interceptación de comunicaciones extranjeras. Se trata de acontecimientos positivos que aún distan de arrojar resultados concretos y que muy probablemente no lo harán durante el mandato del actual titular. Sin embargo, son importantes primeros pasos y el Relator Especial seguirá haciendo todo lo posible para promover y facilitar tales iniciativas.

7. En el presente informe el Relator Especial se centra deliberadamente en las actividades de vigilancia de los organismos del Estado. Para otros ámbitos de actividad, se remite a las líneas de acción temáticas expuestas y descritas en su primer informe a la Asamblea General (A/71/368, párrs. 7 a 17). Cabe destacar que las cuestiones de seguridad y vigilancia se han separado a propósito de la de los datos personales en poder de las empresas y de otras cuestiones, como los macrodatos y los datos abiertos. Estas últimas presentan sus propias dificultades y problemas en relación con el derecho a la privacidad. Se examinan por separado y, de momento, hasta que se integren más adelante en un "enfoque conjunto", seguirán abordándose mediante iniciativas paralelas diferentes establecidas por el Relator Especial. Por ello, el presente informe se centra en las actividades de vigilancia realizadas por el Estado, en su nombre, o a instancias de este.

8. Mientras tanto, la labor sobre las otras líneas de acción temáticas continúa y será presentada en su debido momento, cabe esperar que con arreglo al calendario mencionado en el párrafo 2 del presente informe. En particular, el equipo de tareas sobre macrodatos y datos abiertos está elaborando su primer informe, que se examinará en una sesión de consulta en julio de 2017. Se espera que el resultado de la consulta constituya el tema principal del informe anual que el Relator Especial presentará a la Asamblea General en 2017. Además, tras el éxito del taller sobre privacidad, personalidad y flujos de información celebrado en Nueva York en julio de 2016, el Relator Especial ha comenzado a preparar el segundo taller, que se centrará en el Oriente Medio y el Norte de África. Está previsto que tenga lugar los días 22 y 23 de mayo de 2017 en Túnez y será organizado conjuntamente por el Relator Especial y el organismo de protección de datos de Túnez, en estrecha colaboración con organizaciones de la sociedad civil. También han comenzado los preparativos para el tercer taller, que se centrará especialmente en Asia. Está previsto que se celebre en Hong Kong (China) los días 29 y 30 de septiembre de 2017. Los Gobiernos, organizaciones de la sociedad civil, empresas, organismos de protección de datos, instituciones académicas o los particulares que tengan interés en participar o apoyar estas iniciativas deben ponerse en contacto con el Relator Especial a la mayor brevedad posible[3].

9. El Relator Especial aprovecha esta oportunidad para encomiar a los Gobiernos de Alemania, los Estados Unidos, Francia, el Reino Unido y la República de Corea, por haber respondido de inmediato y positivamente a su solicitud de visita oficial y lamenta la falta de respuesta de varios otros países. Desafortunadamente, puede que esta sea la norma en algunos países, pero es oportuno y necesario señalar a la atención pública la reticencia de los Gobiernos para aceptar solicitudes de visitas al país. El Relator Especial no desea aludir a ningún Gobierno en particular, pero las respuestas o la falta de respuesta a sus solicitudes ayudan a distinguir entre los que se limitan a hablar de los derechos humanos de los que están dispuestos a participar en iniciativas justas para mejorar la protección de la privacidad.

10. Antes de pasar al tema principal del presente informe, el Relator Especial estima necesario señalar una práctica preocupante en algunos Estados que requiere atención urgente e inmediata, y tiene que ver con la utilización de las leyes de privacidad para silenciar al periodismo de investigación. Esto se puede ilustrar mediante casos en que se ha

[3] Para la comunicación por correo electrónico, sírvanse utilizar la dirección srprivacy@ohchr.org o cualquiera de las otras direcciones que figuran en el sitio web del Relator Especial (www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx).

denunciado que los derechos a la privacidad y a la protección de datos han sido erróneamente interpretados por el Ejecutivo y la entidad autónoma nacional para tratar de censurar información contenida en documentos históricos, de manera que se ha impedido el acceso a documentos que datan de hace 30, 40 y hasta 120 años, en clara violación de la libertad de expresión. También se ha denunciado el silencio preocupante de los órganos competentes responsables de la protección del derecho a la privacidad frente a las amenazas contra la privacidad y los intentos claros de las autoridades de censurar información de interés público alegando motivos de protección de datos. El Relator Especial ha establecido buenas relaciones con las autoridades competentes y ha comenzado a examinar esas denuncias, pero aún no ha llegado a una conclusión definitiva sobre su veracidad. Cabe señalar que esta no es la primera ni la única denuncia que ha llegado a su conocimiento de que un Gobierno de un país utiliza la privacidad como excusa para no hacer de dominio público información de interés público. Esta cuestión puede ser objeto de un informe separado y se menciona aquí de manera expresa para invitar a todos, y especialmente a las organizaciones de la sociedad civil, a que denuncien estos casos ante el Relator Especial para que puedan ser investigados en mayor detalle.

11. El Relator Especial celebra que algunos países, como el Brasil, hayan pasado a integrar la familia de naciones que han aprobado leyes nacionales en materia de privacidad y protección de datos, y los alienta a cumplir las normas mínimas, como las establecidas en el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal.

II. Acontecimientos recientes y tendencias preocupantes en las actividades de vigilancia de los organismos del Estado

A. Vigilancia de los organismos del Estado y privacidad en la era digital: *statu quo*

12. El diálogo actual sobre las actividades de vigilancia de los organismos del Estado se ha visto estimulado por personas como Edward Snowden y quienes lo apoyan. Si bien la cuestión es controvertida desde el punto de vista nacional, hay que reconocer que la información divulgada por el Sr. Snowden sobre las prácticas reales de algunos servicios nacionales de seguridad ha abierto un necesario debate sobre lo que significa y lo que debería significar la privacidad en la era digital. Su célebre cita en una entrevista que concedió al periódico *The Guardian*, "No quiero vivir en un mundo donde todo lo que haga y diga quede registrado"[4], ha dado lugar a muchas iniciativas y medidas fundamentales.

13. Las Naciones Unidas han contribuido de diversas maneras al debate sobre las actividades de vigilancia realizadas por el Estado. En su resolución 69/166, la Asamblea General instó a los Estados a que establecieran o mantuvieran mecanismos nacionales de supervisión, de índole judicial, administrativa o parlamentaria, que contasen con los recursos necesarios y fuesen independientes, efectivos e imparciales, así como capaces de asegurar la transparencia, cuando procediera, y la rendición de cuentas por las actividades de vigilancia de las comunicaciones y la interceptación y recopilación de datos personales que realice el Estado. Algunos tribunales regionales de derechos humanos, como el Tribunal Europeo de Derechos Humanos, han emitido fallos que establecen requisitos claros y vinculantes que los Gobiernos deben respetar al establecer los medios para llevar a cabo actividades de vigilancia y en su aplicación[5].

14. El Relator Especial sigue la evolución respecto de la vigilancia del Estado en todo el mundo de varias maneras, entre ellas manteniendo contacto regular con diversas organizaciones nacionales e internacionales de la sociedad civil. Muchas de estas

[4] Disponible en www.theguardian.com/world/2013/jun/09/nsa-whistleblower-edward-snowden-why, consultado el 8 de diciembre de 2016.

[5] Véase, por ejemplo, Tribunal Europeo de Derechos Humanos, *Zakharov v. Russia*, sentencia de 4 de diciembre de 2015. Puede consultarse en: hudoc.echr.coe.int/eng?i=001-159324.

desempeñan un excelente trabajo al señalar a la atención del Relator Especial, de los Gobiernos nacionales y del mundo en general diversas cuestiones preocupantes. Sin desmerecer en modo alguno la labor de otras organizaciones, el Relator Especial quisiera destacar los valiosos esfuerzos realizados por la American Civil Liberties Union[6], Access Now[7], Amnistía Internacional[8], Asociación para el Progreso de las Comunicaciones[9], Article 19[10], Human Rights Watch[11], International Network of Civil Liberties Organizations[12] y Privacy International[13], con las que colabora de diversas formas. Es sumamente beneficioso que estas y otras organizaciones publiquen informes pertinentes, pues el límite de palabras establecido por las Naciones Unidas para los informes oficiales del Relator Especial no le permite incluir descripciones de, por ejemplo, acontecimientos relacionados con la vigilancia, como los que figuran en el informe presentado al Relator Especial por Privacy International en noviembre de 2016 y luego publicado en el sitio web de dicha organización[14]. Es importante señalar que el Relator Especial comparte las preocupaciones de Privacy International sobre acontecimientos relacionados con la vigilancia en Colombia, los Estados Unidos de América, Estonia, la ex República Yugoslava de Macedonia, la Federación de Rusia, Francia, México, Marruecos, Nueva Zelandia, Polonia, el Reino Unido, Rwanda, Sudáfrica, Suecia, Uganda, la República Bolivariana de Venezuela y Zimbabwe, y que sigue de manera independiente la evolución de esos acontecimientos. El Relator Especial invita a los Gobiernos de esos Estados a que tomen nota de las preocupaciones expuestas en los informes de Privacy International y respondan de preferencia públicamente y/o se pongan directamente en contacto con el Relator Especial, según proceda.

15. Sin embargo, es profundamente preocupante que, desde la adopción de la resolución 69/166 y a pesar de las sentencias mencionadas más arriba en el párrafo 13, la situación del derecho a la privacidad en el ámbito de la vigilancia no haya mejorado desde la publicación del informe anterior del Relator Especial. Los Estados que sí reaccionaron comenzaron a trabajar en ello y aprobaron nuevas leyes sobre la materia que solo incluyen, si acaso, leves mejoras en ámbitos limitados. En general, esas leyes han sido redactadas y sometidas a un apresurado proceso legislativo para legitimar prácticas que nunca deberían haberse aplicado.

16. El 21 de diciembre de 2016, el Tribunal de Justicia de la Unión Europea pronunció un fallo muy importante y oportuno en el que recordaba a los Estados miembros de la Unión Europea su obligación de respetar, promover y proteger el derecho humano a la privacidad y otros derechos en la era digital. Con respecto a las obligaciones legales que exigen que los proveedores de servicios de telecomunicaciones conserven datos a gran escala, el Tribunal manifestó que "la injerencia que supone una normativa de este tipo en los derechos fundamentales [...] tiene una gran magnitud y debe considerarse especialmente grave. El hecho de que la conservación de los datos se efectúe sin que los usuarios de los servicios de comunicaciones electrónicas hayan sido informados de ello puede generar en las personas afectadas el sentimiento de que su vida privada es objeto de una vigilancia constante"[15]. También mencionó las posibles consecuencias negativas para el ejercicio de la libertad de expresión.

---

[6] Véase www.aclu.org/issues/national-security/privacy-and-surveillance.

[7] Véase www.accessnow.org/issue/privacy/.

[8] Véase www.amnestyusa.org/our-work/issues/security-and-human-rights/mass-surveillance y www.amnesty.org.uk/issues/Mass-surveillance.

[9] Véase www.apc.org/en/pubs/research.

[10] Véase www.article19.org/cgi-bin/search.cgi?q=privacy.

[11] Véase www.hrw.org/sitesearch/surveillance.

[12] Véase www.inclo.net/.

[13] Véase www.privacyinternational.org/reports.

[14] Privacy International, "Monitoring and oversight of communications surveillance", noviembre de 2016. Puede consultarse en: www.documentcloud.org/documents/3454560-UN-Briefing-Monitoring-and-Oversight-of.html.

[15] Véase Tribunal de Justicia de la Unión Europea, *Tele2 Sverige AB c. la autoridad sueca de control de los servicios de correos y telecomunicaciones*, sentencia de 21 de diciembre de 2016.

17. El Tribunal reconoció asimismo que "si bien es cierto que la eficacia de la lucha contra la delincuencia grave, especialmente contra la delincuencia organizada y el terrorismo, puede depender en gran medida del uso de técnicas modernas de investigación, este objetivo de interés general, por muy fundamental que sea, no puede por sí solo justificar que una normativa nacional que establezca la conservación generalizada e indiferenciada de todos los datos de tráfico y de localización deba ser considerada necesaria a los efectos de dicha lucha"[16]. Además, el Tribunal dejó claro que la conservación de datos de tráfico debe ser la excepción, no la regla. Si hubiera indicios concretos de que esos datos deben conservarse para luchar contra el terrorismo y la delincuencia grave, deben establecerse criterios restrictivos, como limitaciones geográficas precisas. Además, el Tribunal reiteró que las personas afectadas necesitaban medidas de salvaguardia y reparación y que debía haber mecanismos de supervisión efectivos que conllevasen un sistema de control[17].

18. Mientras que, como es comprensible, los defensores de la privacidad celebraron la sentencia, los otros aspectos de la decisión quizás hayan sido resumidos de manera más útil por David Anderson, Letrado de la Corona y Evaluador Independiente de la Legislación contra el Terrorismo del Reino Unido, quien dijo: "La sentencia del Tribunal de Justicia de la Unión Europea fue por tanto verdaderamente radical. La demostrada utilidad de las facultades existentes de retención de datos y los límites que se han impuesto ahora a esas facultades, probablemente signifiquen que habrá motivos de gran preocupación para las fuerzas del orden en el Reino Unido y en otros Estados Miembros. Como contrapeso, no todos coincidirán con la opinión del Tribunal de que dichas facultades constituyen una injerencia 'especialmente grave' en el derecho a la privacidad o que 'pueden generar en las personas afectadas el sentimiento de que su vida privada es objeto de una vigilancia constante' (párr. 100). Un análisis más riguroso de la proporcionalidad se habría centrado en los daños reales que pudiera demostrarse que este útil poder hubiera causado durante sus años de funcionamiento, y habría evitado afirmaciones fundadas en la teoría o en predicciones informales del sentir popular"[18].

19. El Relator Especial procede de una tradición fuertemente comprometida con la formulación de políticas con base empírica, por lo que coincide con el deseo del Evaluador Independiente de que haya un análisis más riguroso de la proporcionalidad. Hasta la fecha, el Relator Especial aún no ha obtenido acceso (por lo menos en el Reino Unido) a ciertos datos (a veces clasificados) que confirmarían que la utilidad de la adquisición de datos a gran escala es necesaria y proporcional al riesgo. De hecho, el Relator Especial acoge con satisfacción la sentencia del Tribunal precisamente porque aún no se ha presentado una prueba que le convenza de que las leyes reguladoras de las actividades de vigilancia que autorizan la adquisición a gran escala de todo tipo de datos, incluidos los metadatos y el contenido, sean proporcionales o necesarias.

20. Es importante señalar los aspectos culturales también indicados por el Evaluador Independiente en este contexto:

"Debe reconocerse, sin embargo, que los sentimientos sobre estas cuestiones sí varían al menos en cierta medida entre los países europeos. Así pues:

- Las observaciones del Tribunal de Justicia de la Unión Europea respecto de la gravedad de la injerencia en la privacidad no se retoman realmente en los tres informes parlamentarios y periciales que dieron lugar a la introducción del proyecto de ley de potestades de investigación, ni en los informes periódicos del Comisionado para la Interceptación de Comunicaciones, ex magistrado superior que realiza la supervisión detallada de esta actividad en el Reino Unido.
- Sin embargo, en la parte oriental de Europa y en Alemania, la experiencia histórica, sumada a una relativa falta de exposición al terrorismo (hasta hace poco) han dado lugar a una mayor circunspección. Las normas nacionales sobre retención de datos se han revelado controvertidas y fueron anuladas incluso antes de la sentencia

[16] *Ibid*.
[17] *Ibid*.
[18] Véase www.terrorismlegislationreviewer.independent.gov.uk/cjeu-judgment-in-watson/.

Digital Rights Ireland en Bulgaria, Rumania, Alemania, Chipre y la República Checa.

Esto puede reflejar lo que he descrito anteriormente como 'marcadas y sistemáticas diferencias de opinión entre los tribunales europeos y los jueces británicos [...], que obedecen al menos a diferentes percepciones de la policía y las fuerzas de seguridad y a conclusiones diferentes (pero igualmente legítimas) que se derivan de la historia del siglo XX en distintas partes de Europa' (*A Question of Trust*, 2.24)"[19].

B. Retos y tendencias preocupantes

21. Mediante diversas actividades de investigación relacionadas con el mandato del Relator Especial y otros proyectos de investigación conexos, se ha determinado que las actividades de vigilancia efectuadas por las fuerzas del orden y por los servicios de seguridad y de inteligencia son cada vez más difíciles de distinguir unas de otras. Mientras que las actividades de las primeras se centran normalmente en la vigilancia dentro de las fronteras del territorio nacional y las de los otros servicios en territorios extranjeros, la naturaleza del flujo transfronterizo de datos y los recursos técnicos necesarios para interceptarlos suelen requerir el uso de equipos idénticos o muy parecidos en la era digital.

22. Cada vez más, los datos personales terminan en la misma "cesta" de datos, que puede utilizarse y reutilizarse para todo tipo de fines conocidos y desconocidos. Ello plantea cuestiones fundamentales en esferas tales como los requisitos para reunir, almacenar, analizar y, en última instancia, eliminar datos. Como ejemplo concreto, en un estudio reciente realizado por el Centro de Privacidad y Tecnología de la Facultad de Derecho de la Universidad de Georgetown, en Washington D.C., se determinó que uno de cada dos estadounidenses adultos figura en un sistema de reconocimiento facial de las fuerzas de seguridad. Los autores del estudio dicen que conocen muy poco de esos sistemas. No saben qué consecuencias tienen para la privacidad y las libertades civiles, ni cómo abordan los problemas de fiabilidad, ni la manera en que alguno de esos sistemas, sean locales, estatales o nacionales, afectan a las minorías étnicas y raciales[20].

23. Estas conclusiones y otras similares conducen a algunas reflexiones. En primer lugar, las características del flujo de datos transfronterizo y la tecnología moderna de la información exigen un planteamiento global de la protección y la promoción de los derechos humanos y particularmente del derecho a la privacidad. Para que la circulación de la información siga siendo un asunto mundial, con todas las importantes ventajas que ha aportado y seguirá aportando a la humanidad, debe haber un entorno coherente y confiable en el que esta se produzca. Ese entorno no puede discriminar entre personas de diferentes naciones, orígenes, razas, sexos, edades, aptitudes, confesiones, etc. Es necesario que haya unos derechos y valores básicos que se respeten, protejan y promuevan sistemáticamente en la comunidad internacional.

24. En segundo lugar, la creciente importancia del intercambio de información en el espacio virtual requiere métodos privados, confiables y seguros. Tecnologías tales como el cifrado ya han sido examinadas ampliamente por el Relator Especial, concretamente en su primer informe a la Asamblea General (véase A/71/368, párrs. 19 a 40). Además, otros titulares de mandatos, como el Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, ya han realizado una labor importante y positiva en este ámbito (véase A/HRC/29/32).

25. Si las fuerzas del orden y los servicios de seguridad y de inteligencia consideran preocupante su incapacidad para interceptar o leer todos los mensajes enviados y recibidos entre personas que usen tecnologías modernas de la información, no deberían olvidar que vivimos en una era en la que la información se intercambia por miles de canales. Los seres humanos han comenzado a intercambiar tanta información a través de medios digitales que, incluso si algunos quedan fuera del alcance del Estado, ello no significa que no existan

[19] *Ibid*.

[20] Clare Garvie, Alvaro Bedoya y Jonathan Frankle, "The perpetual line-up: unregulated police face recognition in America", octubre de 2016. Puede consultarse en www.perpetuallineup.org/.

otras formas de perseguir a quienes lo hacen con malas intenciones. En particular, la ingente cantidad de metadatos generados por los teléfonos inteligentes y otros dispositivos conectados, que a menudo son tan reveladores como el propio contenido de las comunicaciones, ofrecen amplias oportunidades para analizar el comportamiento de las personas[21]. Por otro lado, si el Estado es capaz de interceptar potencialmente todo el flujo de información, incluso retroactivamente mediante la conservación de datos a gran escala y tecnologías como la "congelación rápida" de datos, el derecho a la privacidad sencillamente no experimentará una transición plena a la era digital.

26. Cabe celebrar que algunos países y organizaciones ya hayan comenzado a intensificar sus esfuerzos para afrontar estos retos. El Consejo de Europa, en particular, ha contribuido en este ámbito mediante una iniciativa en el contexto del cumplimiento de la ley en entornos de computación en la nube, que guarda relación con el Convenio sobre la Ciberdelincuencia y tiene por objeto elaborar un nuevo instrumento jurídico[22].

27. Sin embargo, es preocupante que las leyes actuales en materia de vigilancia permitan cada vez más generar y analizar datos personales y acceder a ellos sin la debida autorización y supervisión. El requisito de la autorización y supervisión adecuada debería existir en el momento en que la medida "se ordena, durante su ejecución y después de que esta se ha llevado a cabo"[23]. Mientras que los métodos "tradicionales", como la interceptación de las llamadas telefónicas y de las comunicaciones en general, suelen estar sujetos a autorización judicial, otras técnicas, como la recopilación y el análisis de metadatos relativos a los protocolos del historial de búsquedas en Internet o los datos generados por el uso de teléfonos inteligentes (la ubicación del usuario, las llamadas telefónicas, el uso de las aplicaciones, etc.), están sujetas a salvaguardias mucho menos estrictas. Esto no está justificado, pues la última categoría de datos son por lo menos tan reveladores de la actividad individual de una persona como el contenido real de una conversación. Por lo tanto, deben establecerse salvaguardias adecuadas también para estas medidas.

28. Si bien la autorización judicial de medidas intrusivas por lo general aumenta el grado de protección de la privacidad, también se debe garantizar que los jueces obren con independencia e imparcialidad en los procesos de adopción de decisiones en casos individuales. Asimismo, estos deben disponer del conocimiento y los datos necesarios para examinar exhaustivamente las solicitudes de estas medidas y entender las posibles consecuencias de sus decisiones, en particular respecto de la tecnología que habrá de emplearse y de las consecuencias de usar esa tecnología. Así pues, los Estados deberían impartir la formación requerida y asignar los recursos necesarios para que los jueces estén equipados acometer esta complicada tarea.

29. En principio, lo mismo se aplica para la supervisión de las actividades de vigilancia por órganos especializados de asambleas parlamentarias. No solo deben disponer de la información pertinente para entender las actividades realizadas por las fuerzas del orden y los servicios de seguridad y de inteligencia, sino que también deben tener recursos suficientes para analizarlas y asimilarlas.

30. Esto será difícil de conseguir en la mayoría de los países, debido al gran volumen de datos implicado. Las autoridades que desempeñan actividades de vigilancia deberían tomar medidas para garantizar que las prácticas de supervisión sean revisadas y controladas de manera constante y detallada. La supervisión, sobre todo cuando se efectúa en el ámbito político, debería poder centrarse en cuestiones estructurales y poder abordar la dirección general de las actuaciones.

31. Otra esfera que ha atraído mucha atención es el carácter internacional de las actividades de supervisión. Este fenómeno presenta dos aspectos particulares que requieren

---

[21] Véase, por ejemplo, el informe del Berkman Center for Internet and Society de la Universidad de Harvard, "Don't panic. Making progress on the 'going dark' debate", 2016. Puede consultarse en cyber.harvard.edu /pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_ Debate.pdf.

[22] Véase www.coe.int/en/web/portal/-/cybercrime-towards-a-new-legal-tool-on-electronic-evidence.

[23] Tribunal Europeo de Derechos Humanos, *Zakharov v*. *Russia*.

mayor atención. En primer lugar, es sumamente importante que los Estados respeten el derecho a la privacidad, que se basa en la dignidad humana, a nivel mundial. Las actividades de vigilancia, independientemente de que estén dirigidas a ciudadanos nacionales o extranjeros, únicamente deben llevarse a cabo respetando los derechos humanos fundamentales, como la privacidad. Toda ley nacional o acuerdo internacional que no contemple ese hecho debe considerarse obsoleto e incompatible con el carácter universal de la privacidad y los derechos fundamentales en la era digital.

III. Enfoques iniciales para supervisar de una manera más favorable a la privacidad las actividades de vigilancia de los organismos del Estado

A. Panorama general de los enfoques y los temas

32. La labor de investigación e intercambio de opiniones con diversas autoridades nacionales, la sociedad civil y empresas de distintas regiones del mundo, especialmente durante el Foro Internacional de Supervisión de los Servicios de Inteligencia de 2016, pusieron de manifiesto el surgimiento de varios temas en el ámbito de la vigilancia del Estado. Entre ellas figuran las siguientes:

a) La necesidad de internacionalizar y uniformar la terminología y el lenguaje utilizados;

b) La necesidad de un diálogo franco y confidencial para entender mejor los sistemas nacionales, sus similitudes y diferencias;

c) La promoción y la protección de los derechos humanos fundamentales en relación con los métodos empleados;

d) Las garantías y las vías de reparación, preferentemente en el plano internacional;

e) La rendición de cuentas y la transparencia;

f) La recopilación y el análisis de las buenas y malas prácticas;

g) Un debate más avanzado sobre la manera de estructurar la supervisión de la vigilancia del Estado;

h) Respuestas a la pregunta de cómo colaborar con el público;

i) La necesidad de actuar de manera menos secreta y más proactiva para explicar la labor de vigilancia de los servicios secretos y las fuerzas del orden;

j) La necesidad de contar con más foros para avanzar en esta cuestión.

B. Análisis

33. La finalidad de internacionalizar y uniformar la terminología y el lenguaje es definir términos como “vigilancia”, “vigilancia masiva”, “recopilación de datos a gran escala”, “interceptación a gran escala”, “piratería informática a gran escala”, “interceptación de equipos”, etc. Las autoridades del Reino Unido han publicado un documento útil, aunque controvertido, titulado *Operational case for bulk powers* que propone algunas definiciones de estos términos[24]. Es importante que las autoridades públicas que realizan actividades de vigilancia, la sociedad civil y otras partes interesadas tengan una idea clara de lo que realmente quieren decir cuando emplean términos relativos a la vigilancia. Algunos términos, como “vigilancia masiva”, tienen connotaciones especiales y son muy controvertidos. Lo que se necesita es un uso más completo y armonizado de los términos y

[24] Puede consultarse en: www.gov.uk/government/uploads/system/uploads/attachment_data/file/504187/Operational_Case_for_Bulk_Powers.pdf.

de sus significados en los intercambios entre las autoridades públicas que desempeñan actividades de vigilancia. No obstante, los órganos de supervisión del sistema judicial y político, la sociedad civil, los investigadores del ámbito de la seguridad y las empresas también deberían poder entender y utilizar estos términos adecuadamente.

34. Puesto que la vigilancia tiene una dimensión internacional, es necesario abordar este tema en un foro internacional que sea confidencial y confiable. Es importante que haya más diálogo entre las autoridades nacionales que desempeñan actividades de vigilancia. Asimismo, mientras se mantienen estos diálogos, los expertos de la sociedad civil deben poder hacer aportaciones y compartir sus preocupaciones.

35. Es esencial que los derechos humanos fundamentales, en particular la privacidad, la libertad de expresión y el derecho a la información, sigan ocupando un lugar central en las evaluaciones de las medidas de todo tipo de vigilancia del Estado. Aunque la protección de los derechos a la vida y a la integridad física es una condición básica para la existencia humana, debe tenerse en cuenta que no existe una jerarquía estricta de los derechos humanos. Por lo general se refuerzan mutuamente. Esto significa, dicho de otro modo, que debe haber una amplia promoción de la serie de derechos humanos sin centrarse específicamente en uno o dos derechos.

36. El valor de un derecho solo está determinado por sus delimitaciones y mecanismos de aplicación de la ley. Esto es fundamental en el ámbito de la vigilancia del Estado, ya que hacen falta salvaguardias que trasciendan las fronteras y vías de reparación de carácter transfronterizo. La asistencia judicial, como ya se ha mencionado, debe cumplirse y mejorarse. Si no se puede adoptar un enfoque común a nivel mundial, una posibilidad que aún no se ha descartado, deben adoptarse más iniciativas regionales e interregionales.

37. La estructura respecto de la transparencia y la rendición de cuentas en los organismos públicos que realizan actividades de vigilancia debe ser clara. También deben ser claros los motivos por los que se recopila un determinado conjunto de datos, la finalidad que persigue el análisis y cuáles de sus finalidades no son legales. La aplicación de estos mecanismos debe enmarcarse, ante todo, en los organismos que llevan a cabo actividades de vigilancia, y debe establecerse con claridad quién es responsable del cumplimiento una vez que se hayan definido los requisitos jurídicos adecuados.

38. En este ejercicio es útil reunir ejemplos de buenas y malas prácticas. Por ejemplo, algunos organismos de supervisión de los servicios de inteligencia han establecido órganos de expertos de carácter consultivo integrados por expertos externos de confianza que prestan asesoramiento sobre temas específicos. Además, es esencial realizar evaluaciones de las operaciones y reflexionar sobre sus consecuencias en la promoción y la protección de los derechos humanos fundamentales. También cabe mencionar como un tercer ejemplo que los miembros de los organismos que realizan actividades de vigilancia deben recibir formación para no confiar demasiado en la tecnología y entender que, en definitiva, esta debe ayudar a los humanos a tomar decisiones, y no determinar ese proceso.

39. Si los mecanismos internos de transparencia y rendición de cuentas fallan, es necesario que existan otros sistemas de control. Los Estados deben ser capaces de detectar y evaluar los problemas estructurales en los organismos facultados para realizar tareas de vigilancia. En algunos Estados, estas funciones son ejercidas por comisiones parlamentarias. Sin embargo, las autoridades de supervisión a menudo carecen de conocimientos sobre la materia, de recursos y/o de acceso a información pertinente. Lo mismo ocurre con los mecanismos de control judicial, cuando existen.

40. Además, la información revelada por Snowden, y sus repercusiones, han demostrado claramente que hay una necesidad acuciante de que las autoridades públicas expliquen su labor. Ello puede lograrse parcialmente mediante la notificación *a posteriori* de las personas que son objeto de vigilancia. Cuando eso pueda hacerse en condiciones seguras, se debería dar noticia a esas personas y explicar las consecuencias de esas operaciones. Esas personas también deberían tener derecho a modificar o eliminar información personal no pertinente, siempre y cuando esa información ya no sea necesaria para llevar a cabo una investigación en curso o pendiente para la que se haya autorizado debidamente su recopilación y uso.

41. Además, la población general debe volver a confiar en la labor de los organismos encargados de la vigilancia. Es evidente que la seguridad es una preocupación legítima para todo el mundo. Por lo tanto, aunque no hace falta que la población en general entienda en detalle las características y las aplicaciones de todas y cada una de las operaciones, la información debe estar disponible para que se pueda entender la dimensión general de las operaciones efectuadas para proteger a la población. Un pasajero no necesita saber pilotar un avión para reservar un vuelo, pero no comprará el pasaje si no confía en la capacidad general y la seguridad del de tráfico aéreo y los sistemas de seguridad.

IV. Actividades del Relator Especial

42. El Relator Especial sobre el derecho a la privacidad presenta informes acerca de las principales actividades públicas o semipúblicas realizadas como parte de su mandato. El presente informe recoge las actividades realizadas entre julio de 2016 y principios de febrero de 2017. Son las siguientes:

a) Seminario europeo sobre innovación en la protección de la privacidad, Centro de Investigación de Huawei en Alemania, celebrado en Múnich (Alemania) el 3 de agosto de 2016;

b) Orador principal en una conferencia del Consejo de Europa titulada “Libertad de internet: un factor constante de la seguridad democrática en Europa”, celebrada en Estrasburgo (Francia) el 9 de septiembre de 2016;

c) Presidente de una mesa redonda sobre biometría y privacidad en una conferencia sobre proyectos de investigación de la Asociación Europea de Biometría, celebrada en Darmstadt (Alemania) los días 19 y 20 de septiembre de 2016;

d) Reunión del Grupo Asesor sobre Protección y Seguridad de la Iniciativa Horizonte 2020, Dirección General de Migración y Asuntos de Interior de la Comisión Europea, celebrada en Bruselas el 27 de septiembre de 2016;

e) Foro Internacional de Supervisión de los Servicios de Inteligencia, en calidad de Relator Especial, celebrado en Bucarest los días 11 y 12 de octubre de 2016;

f) Orador principal y presidente de una mesa redonda en la Conferencia sobre la Inteligencia en la Sociedad del Conocimiento, celebrada en Bucarest los días 13 y 14 de octubre de 2016;

g) Orador principal en la 38ª Conferencia Internacional de Autoridades de Protección de Datos y Privacidad, celebrada en Marrakech (Marruecos) del 18 al 22 de octubre de 2016;

h) Segunda asamblea general anual de MAPPING, celebrada en Praga del 31 de octubre al 2 de noviembre de 2016;

i) Orador principal en la Conferencia sobre el Ciberespacio celebrada en Brno (Chequia) los días 25 y 26 de noviembre de 2016;

j) Orador principal en el Foro de Autoridades de Privacidad Asia-Pacífico, celebrado en Manzanillo (México) del 30 de noviembre al 2 de diciembre de 2016;

k) Orador principal e integrante de una mesa redonda en un simposio sobre vigilancia del Irish Council for Civil Liberties, celebrado en Dublín el 7 de diciembre de 2016;

l) Orador principal en la presentación del informe anual de la Comisión de Derechos Humanos de Irlanda del Norte, celebrada en Belfast (Reino Unido) el 8 de diciembre de 2016;

m) Reuniones preparatorias para el segundo seminario sobre la privacidad, la personalidad y la libre circulación de la información, celebrado en Túnez del 12 al 14 de diciembre de 2016;

n) Integrante de una mesa redonda sobre inteligencia artificial y privacidad en la décima Conferencia Internacional sobre Computadoras, Privacidad y Protección de Datos, celebrada en Bruselas del 25 al 27 de enero de 2017;

o) Orador principal sobre privacidad y seguridad en la novena edición del Foro de la Privacidad, Asociación Española para el Fomento de la Seguridad de la Información, ISMS Forum Spain, celebrado en Madrid los días 1 y 2 de febrero de 2017.

V. Conclusiones y recomendaciones

43. **En esta etapa, el Relator Especial desea formular cinco recomendaciones concretas que se derivan de sus conclusiones provisionales. Abordan las siguientes cuestiones:**

a) Motivos por los que el populismo y la privacidad son perjudiciales para la seguridad;

b) Formas de colaboración de los Estados para aumentar la protección de la privacidad mediante una mejor supervisión de los servicios de inteligencia;

c) Quién merece disfrutar del derecho a la privacidad, esto es, todos en todas partes; la universalidad del derecho a la privacidad cobra un significado especial en este contexto;

d) Maneras en que el derecho a la privacidad podría protegerse mejor mediante modificaciones en las leyes nacionales y el derecho internacional;

e) Momento en que determinados avances en el derecho internacional, especialmente en relación con un instrumento normativo que regule las actividades de vigilancia, podrían estar en una etapa lo suficientemente avanzada para permitir un debate más amplio.

Motivos por los que el populismo y la privacidad son perjudiciales para la seguridad

44. **Para ser más precisos esta sección debería tal vez titularse seguridad, populismo y privacidad. Entre 2015 y 2017 se ha registrado una tendencia cada vez mayor, sobre todo, aunque no exclusivamente, en Europa, a complacerse en la "política de gestos". Dicho de otro modo, en los últimos 18 meses ha habido políticos que, para mostrar que hacen algo por la seguridad, sancionan leyes que establecen facultades que invaden la privacidad —o legitiman prácticas existentes— sin demostrar en modo alguno que sean proporcionales o, de hecho, eficaces para combatir el terrorismo.**

45. **Las leyes que se han aprobado recientemente se basan en una psicología del miedo: el miedo desproporcionado, aunque comprensible, que pueden tener los votantes ante la amenaza del terrorismo. El miedo impide que los votantes evalúen objetivamente la eficacia de las medidas propuestas.**

46. **Hay muy pocas pruebas, o ninguna, que persuada al Relator Especial de la eficacia o la proporcionalidad de algunas de las medidas sumamente invasivas de la privacidad de las personas introducidas por las nuevas leyes en materia de vigilancia en Alemania, los Estados Unidos, Francia y el Reino Unido. Al igual que el juez que se pronunció en una causa reciente acerca del veto migratorio en los Estados Unidos, el Relator Especial debe buscar pruebas que demuestren la proporcionalidad de las medidas previstas en las leyes[25]. Así, de la misma manera en que el juez preguntó exactamente cuántos actos de terrorismo habían sido cometidos desde 2011 por nacionales de los Estados afectados por el veto migratorio, el Relator Especial debe preguntar si no sería mucho más proporcional, por no hablar de más rentable y menos lesivo para la privacidad, invertir más dinero en los recursos humanos**

[25] Véase www.npr.org/2017/02/04/513446463/who-is-judge-james-l-robart-and-why-did-he-block-trumps-immigration-order.

necesarios para efectuar actividades concretas de vigilancia e infiltración y gastar menos esfuerzo en la vigilancia electrónica. Todo ello en un momento en que la gran mayoría de los ataques terroristas han sido cometidos por individuos que ya estaban fichados por las autoridades.

47. **También hay cada vez más pruebas de que la información que obra en poder de los Estados, entre otra la información obtenida a gran escala o mediante actividades de vigilancia masiva, es cada vez más susceptible de ser pirateada por Gobiernos hostiles u organizaciones delictivas. En ninguna parte se ha demostrado que el riesgo creado por la reunión de esos datos sea proporcional a la reducción del riesgo conseguida mediante la obtención de datos a gran escala.**

48. **Además, el abuso en cuanto a la recopilación de datos mediante la adquisición a gran escala sigue siendo un motivo de preocupación primordial. Sin que ello implique necesariamente una crítica a la nueva administración de los Estados Unidos, cabe reproducir aquí las preocupaciones expresadas en este sentido por un investigador superior de Human Rights Watch: "En los Estados Unidos, el Organismo Nacional de Seguridad sigue recopilando información de forma indiscriminada sobre millones de personas todos los días, a pesar de modestas reformas en 2015. Las llaves del sistema de vigilancia más sofisticado del mundo han pasado a manos de [...] un candidato [que] amenazó con encarcelar a su adversaria política, registrar y vetar a los musulmanes, deportar a millones de inmigrantes y atacar la libertad de prensa"[26]. Aunque cabe esperar que el sistema de equilibrio de poderes de los Estados Unidos o, de hecho, los principios éticos del propio poder ejecutivo puedan alejar al país de la materialización de estos riesgos, lo que el Relator Especial quiere señalar es que, una vez que existen conjuntos de datos obtenidos por medio de actividades de vigilancia masiva o adquisición a gran escala y un nuevo Gobierno carente de escrúpulos asume el poder en cualquier parte del mundo, la posibilidad de que se haga un uso indebido de esos datos es tal que directamente pone en cuestión la propia recopilación.**

49. **Por lo tanto, el Relator Especial recomienda a los Estados que desistan de apelar al miedo y aumenten la seguridad adoptando medidas proporcionales y eficaces, y no mediante leyes que invaden la privacidad y que son indebidamente desproporcionadas. Como dijo el Cardenal Vincent Nichols, arzobispo de Westminster: "No creo que ninguna forma de liderazgo se vea favorecida por el uso del miedo. El verdadero liderazgo político no se aprovecha del miedo"[27].**

Formas de colaboración de los Estados para aumentar la protección de la privacidad mediante una mejor supervisión de los servicios de inteligencia

50. **El Foro Internacional de Supervisión de los Servicios de Inteligencia de 2016 demostró que el debate sobre la manera de gestionar la supervisión de los servicios de inteligencia de modo que se refuercen las garantías de privacidad es un proceso complejo que requiere mucho tiempo, recursos, eventuales cambios culturales, voluntad política y generación de confianza. No hay atajos para identificar y seguir desarrollando las mejores prácticas.**

51. **La recomendación del Relator Especial es sencilla pero importante: todos los Estados Miembros de las Naciones Unidas deberían participar en el minucioso debate sobre la supervisión de los servicios de inteligencia iniciado por el Relator Especial en el Foro Internacional de Supervisión de los Servicios de Inteligencia de 2016, que proseguirá en el Foro de 2017. Los Gobiernos deberían alentar a los órganos de supervisión y los servicios de inteligencia a que participen en los Foros y facilitar su participación.**

[26] Cynthia M. Wong, "Surveillance in the age of populism", Human Rights Watch, febrero de 2017. Puede consultarse en: www.hrw.org/news/2017/02/07/surveillance-age-populism.

[27] Declaraciones del Cardenal Vincent Nichols en el programa de la BBC Radio 4, *The Westminster Hour*, el 5 de febrero de 2017.

Quién merece disfrutar del derecho a la privacidad

52. **El Relator Especial recomienda a los Estados que estén dispuestos a garantizar que, tanto a nivel nacional como internacional, la privacidad sea respetada como un derecho auténticamente universal y que, sobre todo en lo que respecta a la vigilancia en Internet, no sea o deje de ser un derecho en función del pasaporte de cada quien.**

53. **El desarrollo de esta recomendación requiere cierto espacio y se ilustrará utilizando ejemplos que aquí se limitarán (estrictamente por razones de espacio) a la jurisprudencia y las reformas legislativas de los Estados Unidos. Debe quedar claro desde un principio que todo lo que aquí se recomienda a los Estados Unidos se recomienda igualmente en situaciones análogas a todos los Estados Miembros de las Naciones Unidas.**

54. **El 6 de febrero de 2017, la Cámara de Representantes de los Estados Unidos hizo algo muy loable que el Relator Especial aguardaba desde hacía mucho tiempo. Aprobó por unanimidad la Ley de Privacidad de los Correos Electrónicos, que colmó una laguna en la legislación de los Estados Unidos al exigir una orden judicial para permitir el acceso a los correos electrónicos de más de seis meses de antigüedad almacenados en la nube u otros sitios. El Relator Especial acoge con gran satisfacción este acontecimiento y confía en que la Ley sea aprobada también en el Senado, que frustró el proceso la última vez que se intentó en abril de 2016. De hecho, el Relator Especial invita al Senado a que aproveche esta histórica oportunidad y dé un paso más allá, demostrando así el compromiso de los Estados Unidos con los derechos humanos en el mundo entero y, al mismo tiempo, poniendo fin a una de las falacias xenófobas que algunos Gobiernos promueven consciente o inconscientemente, a saber, que los "despreciables extranjeros nos perjudican" y que, por tanto, no merecen que sus derechos humanos fundamentales sean protegidos por la ley.**

55. **Esta no es una deficiencia exclusiva de algunas disposiciones legislativas de los Estados Unidos. Por ejemplo, el Gobierno de Alemania ha incurrido en la misma falta al adoptar recientemente una ley que distingue entre los ciudadanos alemanes y de la Unión Europea, por un lado, y todos los demás, por otro (véase A/71/368, párrs. 35 y 36). Por supuesto, estas leyes podrían refutarse basándose meramente en la lógica: la inmensa mayoría de los atentados terroristas en Europa no fueron cometidos por extranjeros, sino principalmente por ciudadanos de la Unión Europea que tenían documentos de identidad y pasaportes de la Unión Europea. Del mismo modo, parece que la situación es la misma en la mayoría de los recientes atentados terroristas en los Estados Unidos. Entonces, ¿por qué consentir el falaz argumento de que es lógico y razonable discriminar a quienes no tengan la misma ciudadanía que los legisladores? Si los Gobiernos realmente quieren prevenir y combatir el terrorismo, el sentido común sugiere que deben abordar las causas profundas del problema, como la radicalización. Invertir mucho más en las medidas destinadas a combatir la radicalización y asignar más recursos para actividades de vigilancia selectiva a largo plazo e infiltración en células terroristas parecería mucho más eficaz que complacerse en políticas de gestos. Es evidente que tratar de parecer inflexibles en cuestiones de seguridad legitimando medidas en gran medida inútiles, sumamente caras y totalmente desproporcionadas que invaden la privacidad de tantas personas —y otros derechos— no es el camino que los Gobiernos deberían seguir.**

56. **El Relator Especial sugiere con todo respeto que sería mucho más sensato y eficaz, y además serviría de ejemplo para el resto del mundo, que la legislación de los Estados Unidos se alineara con los principios formulados recientemente en Europa por el Tribunal Europeo de Derechos Humanos en el asunto *Zakharov c. Rusia,* y por el Tribunal de Justicia de la Unión Europea en *Tele 2 Sverige AB c. la autoridad sueca de control de los servicios de correos y telecomunicaciones*, concretamente que el requisito fundamental para efectuar actividades de vigilancia selectiva es la sospecha fundada y no la nacionalidad. Si los servicios de seguridad y de inteligencia o las fuerzas del orden pueden demostrar que existe una sospecha fundada, se les debe conceder la autorización judicial para obtener una orden de acceso, independientemente de la nacionalidad del sospechoso. La principal consideración es y debería seguir siendo la gestión del riesgo. Si se demuestra que una persona**

constituye un riesgo, debería ser sometida a vigilancia en todo lugar y momento, independientemente del pasaporte que tenga. Las mismas garantías que se aplican contra los registros e incautaciones indebidos —en este caso una orden judicial—son apropiadas en estos casos, independientemente de la nacionalidad de las personas. En la Declaración Universal de Derechos Humanos no se afirma, con toda razón, que solo los ciudadanos de los Estados Unidos tienen derecho a la privacidad. En cambio, dice que toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques (véase el art. 12), lo cual, según entiende el Relator Especial, incluye también a las leyes de los Estados Unidos. Por tanto, esta es una oportunidad para que los legisladores de los Estados Unidos den ejemplo a otros en todo el mundo, cumplan con el espíritu y la letra de la Declaración Universal y tomen medidas concretas para que la legislación de los Estados Unidos respete verdaderamente la universalidad del derecho a la privacidad, modificando la Ley de Privacidad de los Correos Electrónicos de las maneras adecuadas, algunas de las cuales se exponen a continuación.

57. **Si la privacidad, como el derecho a no ser torturado o tantos otros derechos, es un derecho humano fundamental, también es un derecho universal, lo que significa que todas las personas en todo el mundo tienen derecho a la privacidad, independientemente del lugar en que se encuentren, del pasaporte que tengan y de su color, credo, origen étnico, filosofía política u orientación sexual. El Relator Especial pide también al Senado de los Estados Unidos que suscriba esta realidad. En muchas ocasiones, los Gobiernos de los Estados Unidos han procurado sancionar las violaciones de los derechos humanos en otros países, y a menudo han sido los primeros en trazar líneas rojas y establecer sanciones para aumentar las posibilidades de que se respeten. Si eliminara la distinción entre los ciudadanos estadounidenses y los de otros países extendiendo las garantías de privacidad de que gozan los ciudadanos de los Estados Unidos a todos los ciudadanos del mundo, el Senado se posicionaría de manera clara a favor de la universalidad del derecho humano fundamental a la privacidad y en contra de las tendencias xenófobas en la elaboración de las leyes. Con ello, también estaría en consonancia con las leyes en materia de privacidad y protección de datos de la Unión Europea y el Consejo de Europa, que no distinguen entre el derecho a la privacidad de los ciudadanos y los no ciudadanos.**

Maneras en que el derecho a la privacidad podría protegerse mejor mediante modificaciones en las leyes nacionales y el derecho internacional

58. **Mientras que la recomendación anterior trata principalmente de las posibilidades de proteger la universalidad de la privacidad en el ordenamiento jurídico interno, en los párrafos siguientes se exponen las posibilidades de complementar las medidas nacionales mediante el derecho internacional.**

59. **Otra preocupación fundamental que suscita la versión actual del texto de la Ley de Privacidad de los Correos Electrónicos de los Estados Unidos es si las garantías que la Ley refuerza se aplican también a los datos, independientemente del lugar donde estén almacenados, sea en los Estados Unidos o en otras partes. Para ilustrar esta cuestión, cabe citar la demanda interpuesta por Microsoft en la que impugna el alcance mundial de las órdenes de registro de los Estados Unidos relativas a los datos almacenados fuera del país[28]. Se puede entender fácilmente la renuencia de Microsoft a otorgar acceso a los datos almacenados fuera de los Estados Unidos. No solo porque puede afectar la competitividad de la propia empresa en todo el mundo, sino también porque supondría un problema particularmente arduo al tratar de decidir cómo abordar todo tipo de solicitudes de datos cursadas por todo tipo de Gobiernos de todo el mundo. Este no es un problema exclusivo de Microsoft. La mayoría de los otros gigantes tecnológicos, en su mayoría empresas estadounidenses, como Google, Facebook, Apple y Twitter (por nombrar solo algunas), reciben todos los años miles de solicitudes de Gobiernos de todo el mundo para acceder a datos.**

[28] Véase blogs.microsoft.com/on-the-issues/2016/07/14/search-warrant-case-important-decision-people-everywhere/#sm.0019d8sjw1492dnrz7k1yawh09b46.

60. **Si el Congreso de los Estados Unidos desea encontrar una manera sensata de avanzar en este aspecto, por no decir ya una solución que sea adecuada desde la perspectiva de los derechos humanos fundamentales y que no ponga a las empresas estadounidenses en una situación de desventaja comercial, debe caer en la cuenta de que la respuesta no puede radicar únicamente en la legislación nacional. También debe comprender que este ámbito del derecho no está bien cubierto por mecanismos tales como la asistencia judicial, que existen desde hace decenios. El Congreso debe entender que, si bien el Convenio sobre la Ciberdelincuencia logró importantes avances en algunos ámbitos, aún no ha conseguido que la transferencia de datos personales a través de las fronteras y el acceso a los datos necesarios para las investigaciones sea tan rápida y tan exenta de problemas como algunos hubieran esperado. Una de las principales razones de ese relativo fracaso es que ha seguido basándose en exceso en el concepto del Estado nación soberano del siglo XIX, en vez de atender a la realidad de la Internet sin fronteras del siglo XXI. Aunque tal vez el Convenio sea un buen ejemplo de lo que puede conseguirse dando pequeños pasos, y sin duda ha tenido algunos resultados positivos, como la identificación y la codificación de los delitos cometidos con tecnología informática o en Internet, no ha conseguido generar oportunamente flujos transfronterizos de datos personales que sean apropiados para detectar, investigar y prevenir delitos en la era de internet. Una de las posibles razones principales de que no lo haya hecho es que no se dio el otro paso necesario para crear un mecanismo, por ejemplo un organismo internacional encargado de permitir el acceso internacional a los datos y con la autoridad para hacerlo.**

61. **De la misma manera que otros instrumentos de derecho internacional han establecido organismos encargados de generar confianza y aplicar salvaguardias adecuadas en ámbitos tan diversos como el derecho marítimo, el derecho espacial, las armas atómicas o las armas químicas, entre otros, el Convenio sobre la Ciberdelincuencia, junto con otros tratados multilaterales, incluidos algunos nuevos creados con ese fin, tiene la posibilidad de ampliarse para establecer una autoridad internacional que esté facultada para emitir lo que sería el equivalente de una orden internacional de vigilancia o una orden internacional de acceso a los datos ejecutable en el ciberespacio. Los países firmantes de ese nuevo tratado, o de un protocolo adicional podrían aportar sus propios jueces independientes especializados para crear un cuerpo de magistrados que, conformado como un tribunal, podría perfectamente actuar como instancia única para la emisión de las correspondientes órdenes judiciales ejecutables en todo el mundo —en todos los países que sean parte en el tratado. De esta manera, volviendo al ejemplo anterior de la resolución de julio de 2016 sobre el caso de Microsoft, las empresas como Microsoft, Google, Facebook, Amazon, Apple y otros gigantes tecnológicos que administran centros de datos en el plano internacional no tendrían que preocuparse por que un Estado se excediera en sus atribuciones, sino que, en cambio, estarían frente a una orden internacional de acceso a los datos emitida por motivos de sospecha razonable con arreglo a una norma de derecho internacional clara. De igual modo, los ciudadanos de todo el mundo tendrían la certeza de que su derecho a la privacidad, además de otros derechos, como la libertad de expresión y de asociación, estarían protegidos por salvaguardias apropiadas, de una manera igualitaria y universal. Si realmente queremos que el derecho a la privacidad sea universal, parece lógico afirmar que se puede avanzar en esa dirección mediante mecanismos que sean a la vez internacionales y universales y que apliquen las mismas normas y salvaguardias en todo el mundo.**

62. **Esto no es una utopía. Es la pura y dura realidad, algo que diferenciará a las verdaderas democracias de los Estados que principalmente intentan utilizar Internet como un medio de control social y de retener el poder en sus propios territorios. También es algo que podría asociarse con otras iniciativas destinadas a preservar la paz informática, como ha propuesto recientemente el Presidente y Oficial Jurídico Principal de Microsoft[29].**

63. **En la actualidad, las pruebas de que dispone el Relator Especial indicarían que, lamentablemente, algunos Estados, incluso algunas de las principales democracias, conciben internet de una manera oportunista como un espacio en el que sus fuerzas del orden y, especialmente, sus servicios de seguridad y de inteligencia, pueden actuar relativamente sin obstáculos, interceptando datos e interviniendo millones de dispositivos (teléfonos inteligentes, tabletas y computadoras portátiles, así como servidores) en todo el mundo. Así, entre 15 y 25 Estados emplean Internet como si fuera su propio campo de juego en el que pudieran disputarse el botín, siempre buscando sacar ventaja, ya sea en lo que respecta a la ciberguerra, el espionaje y el contraespionaje, o el espionaje industrial. La lista de motivos es larga, mientras que otros aproximadamente 175 Estados observan con impotencia, sin mucho que hacer más que confiar en que la paz informática prevalecerá de alguna manera.**

64. **Para decirlo con franqueza, una minúscula minoría de Estados ha intentado de manera activa y oficiosa disuadir al Relator Especial de que examine opciones para encontrar soluciones en este ámbito, pero su obligación es informar de que esas parecen ser las únicas personas que no desean que haya garantías y vías de reparación exigibles en el plano internacional con respecto a Internet. Todavía no he encontrado ninguna organización de la sociedad civil, empresa o incluso organismo de mantenimiento del orden o servicio de seguridad o de inteligencia razonables que no deseen tener mayor claridad y garantías y vías de reparación universalmente aplicables, por más que puedan dudar de que ello pueda conseguirse en el corto plazo.**

65. **La única forma de conseguir esa claridad e introducir esas garantías y vías de reparación de manera que su aplicación sea más oportuna, imparcial y apropiada es mediante acuerdos multilaterales consagrados en el derecho internacional. Lo que el mundo necesita no son más prácticas reprobables en Internet auspiciadas por los Estados, sino acuerdos racionales y civilizados sobre el comportamiento adecuado de los Estados en el ciberespacio, lo que lleva de nuevo al presente informe a la cuestión de la vigilancia.**

66. **Algunos de los mecanismos internacionales ampliados que se han mencionado anteriormente serían muy útiles para hacer cumplir la ley en el ciberespacio, lo cual está regulado actualmente por el Convenio sobre la Ciberdelincuencia. Sin embargo, como su nombre sugiere, el Convenio, que ya ha sido suscrito por un 25% de los Estados Miembros de las Naciones Unidas, se ocupa únicamente del sector de la justicia penal. No se ocupa de la seguridad nacional ni de la vigilancia efectuada en nombre de la seguridad nacional. En otras palabras, el tipo de actividades reveladas por Edward Snowden queda fuera del alcance del Convenio, y para poder regularlas satisfactoriamente, se debería ampliar considerablemente el alcance del Convenio o aprobar un tratado distinto, pero complementario, que regule adecuadamente las actividades de vigilancia en el ciberespacio. Eso sería mucho más deseable que una situación en la que algunas democracias, como Alemania, los Estados Unidos, Francia y el Reino Unido, están haciendo esfuerzos denodados por introducir de nuevas leyes para regular las actividades de vigilancia y en la que la mentalidad parece estar influenciada sobremanera por el concepto de Estado nación soberano del siglo XIX.**

67. **Si bien el nacionalismo y el patrioterismo, por no mencionar el populismo, parecen estar experimentando lo que podría ser en la historia un aumento cíclico, su eficacia en las urnas no debe confundirse con su capacidad para proporcionar una seguridad efectiva, tanto a nivel nacional como internacional. Debe reconocerse**

[29] Véase: www.itpro.co.uk/security/28134/how-can-nation-states-win-the-unfolding-cyberwar?_mout=1&utm_campaign=newsletter&utm_medium=email&utm_source=newsletter&tpid=109380765640.

—incluso por los políticos en el ámbito nacional— que la gran mayoría de los Estados Miembros no tiene ningún interés en promover actos de delincuencia organizada o de terrorismo, donde sea que puedan ocurrir y sean quienes sean los autores. Para decirlo sencillamente, si un investigador en Bélgica acudiera a un tribunal internacional conformado por jueces de, digamos, Alemania, el Brasil, los Estados Unidos, Francia, Ghana, la India y el Reino Unido —por mencionar algunos países al azar—, no debería temer que tal tribunal, o uno conformado de manera similar para ese fin, no concediera una orden para acceder a los datos de una persona si se demostrara una sospecha fundada. Una vez que el proceso conduce a una orden internacional de acceso a los datos, se simplificarían considerablemente las cosas para los Gobiernos y las empresas dentro de las jurisdicciones de los Estados que han adoptado ese mecanismo mediante un tratado internacional.

68. **Dicho instrumento normativo no debe confundirse con un tratado exhaustivo sobre la gobernanza de Internet, o un "Convenio de Ginebra para Internet", como algunos lo han llamado. Hay muchos otros aspectos de la gobernanza de Internet que no se verían afectados por un instrumento jurídico que regule las actividades de vigilancia en el ciberespacio, entre los que cabe destacar un aspecto muy importante, y frecuentemente ignorado, del artículo 12 de la Declaración Universal de Derechos Humanos y el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, concretamente el derecho a la protección de la reputación, que es un derecho distinto pero similar al derecho a la privacidad.**

Momento en que determinados avances en el derecho internacional, especialmente en relación con un instrumento normativo que regule las actividades de vigilancia, podrían estar en una etapa lo suficientemente avanzada para permitir un debate más amplio

69. **En síntesis, un instrumento jurídico que regule las actividades de vigilancia en el ciberespacio sería una medida complementaria a otros instrumentos del derecho cibernético existente, como el Convenio sobre la Ciberdelincuencia, y podría contribuir considerablemente a la provisión de garantías concretas para la privacidad en Internet. Felizmente para el mandato del Relator Especial, en el marco de una iniciativa ya existente, el proyecto sobre alternativas de gestión en materia de privacidad, propiedad intelectual y gobernanza de internet (proyecto MAPPING), que cuenta con el apoyo de la Unión Europea, se están estudiando opciones para un instrumento jurídico que regule las actividades de vigilancia en el ciberespacio. Hay un proyecto de texto que está siendo debatido por expertos de la sociedad civil y algunas de las mayores empresas internacionales y está previsto que se dé a conocer al público en algún momento de 2017, sin duda antes de la primavera de 2018. Sería precipitado que cualquier persona, incluido el Relator Especial, emitiera un juicio sobre dicho texto, o uno similar, en esta etapa preliminar en que se están estudiando las opciones, pero es posible que finalmente se revele como un útil punto de partida para que los Gobiernos dialoguen en el marco de las organizaciones intergubernamentales, entre otras, y tal vez especialmente, las Naciones Unidas.**

70. **De la misma manera en que el Relator Especial se está preparando para examinar este tema, particularmente entre marzo y julio de 2018, parecería razonable que los poderes ejecutivos de muchos países recibieran un mandato de sus parlamentos —y de sus votantes, en los casos en que se celebren elecciones en 2017 y 2018— para considerar de manera activa esas opciones para regular debidamente las actividades de vigilancia e introducir garantías y vías de reparación favorables a la privacidad en el ciberespacio. Ello no solo tendría un gran valor intrínseco para los ciudadanos de todo el mundo, sino que también enviaría una clara señal a los Estados, las democracias, las pseudodemocracias y demás regímenes que creen erróneamente que la mejor manera de proceder en relación con el ciberespacio es reclamar soberanía sobre una parte de Internet o sobre lo que sus ciudadanos hacen en la red. Los derechos humanos son universales y el derecho cibernético debería proteger no solo la privacidad, sino también otros derechos humanos fundamentales.**

71. **Por más que pueda resultar difícil conseguirlo, no es imposible; de hecho, es plausible y razonable que un número considerable de Estados puedan llegar finalmente a unirse en torno a un instrumento jurídico que regule las actividades de vigilancia y proteja la privacidad en el ciberespacio. Ello sería positivo para los ciudadanos, los Gobiernos, la privacidad y las empresas. El número de Estados que se adhiera a los nuevos principios y mecanismos podría aumentar gradualmente hasta conformar una masa crítica. Esa ha sido la enseñanza extraída de la evolución del derecho internacional en los últimos dos siglos. No hay ninguna razón para ignorar esa enseñanza en lo que respecta a la privacidad, la vigilancia y el ciberespacio. Quizás no se concrete durante el mandato del Relator Especial, pero es al menos la vía posiblemente más prometedora por la que comenzar. Todo lo que el Relator Especial ha observado durante su mandato hasta el día de la fecha lo ha persuadido de que esta puede ser la vía más sensata que haya que tomar cuando llegue el momento. Ese momento puede estar más cerca de lo que algunos quisieran pensar.**