Naciones Unidas A/69/397

Asamblea General

Distr. general
23 de septiembre de 2014
Español
Original: inglés

Sexagésimo noveno período de sesiones
Tema 68 a) del programa
Promoción y protección de los derechos humanos: aplicación de los instrumentos de derechos humanos

Promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo*

Nota del Secretario General

El Secretario General tiene el honor de transmitir a la Asamblea General el informe del Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, Sr. Ben Emmerson, presentado de conformidad con la resolución 68/178 de la Asamblea General y la resolución 15/15 del Consejo de Derechos Humanos.

* Documento presentado con retraso.

14-61490 (S) 131014 141014

Informe del Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo

Resumen

Este es el cuarto informe anual que presenta a la Asamblea General el actual Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, Sr. Ben Emmerson.

Las principales actividades llevadas a cabo por el Relator Especial entre el 17 de diciembre de 2013 y el 31 de julio de 2014 se enumeran en la sección II del informe. En la sección III, el Relator Especial examina el uso de la vigilancia digital a gran escala en la lucha contra el terrorismo, y analiza los efectos del uso de la tecnología de acceso masivo en el derecho a la privacidad consagrado en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos.

I. Introducción

1. El Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, Sr. Ben Emmerson, presenta este informe a la Asamblea General de conformidad con su resolución 68/178 y las resoluciones 15/15, 19/19, 22/8 y 25/7 del Consejo de Derechos Humanos. En el informe se describen las actividades llevadas a cabo por el Relator Especial entre el 17 de diciembre de 2013 y el 31 de julio de 2014. Además, se examina el uso de la vigilancia digital a gran escala en la lucha contra el terrorismo, y se analizan los efectos del uso de la tecnología de acceso masivo en el derecho a la privacidad consagrado en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos.

II. Actividades relacionadas con el mandato

2. El 13 de febrero de 2014, el Relator Especial participó como ponente en una mesa redonda denominada “Debate sobre *Kadi II*: el Ombudsman de las Naciones Unidas y la revisión judicial en el proceso de adopción de decisiones sobre sanciones del Consejo de Seguridad”, que tuvo lugar en la London School of Economics, en Londres.

3. Del 23 al 25 de febrero de 2014, el Relator Especial participó en un seminario de expertos en Ginebra sobre “El derecho a la privacidad en la era digital”, auspiciado por las Misiones Permanentes de Alemania, Austria, Brasil, Liechtenstein, México, Noruega y Suiza en Ginebra, y organizado por la Academia de Derecho Internacional Humanitario y Derechos Humanos de Ginebra.

4. El 11 de marzo de 2014, el Relator Especial presentó al Consejo de Derechos Humanos, en su 25º período de sesiones, un informe sobre el uso de aeronaves teledirigidas, o drones, en operaciones letales extraterritoriales de lucha contra el terrorismo, en particular en el contexto de conflictos armados asimétricos, y sus consecuencias para la población civil (A/HRC/25/59). También mantuvo un diálogo interactivo con el Consejo sobre sus informes relativos a las visitas que realizó a Burkina Faso (A/HRC/25/59/Add.1) y Chile (A/HCR/25/59/Add.2).

5. El 12 de marzo de 2014, el Relator Especial participó como ponente en una reunión paralela sobre “Los derechos humanos y los drones” y celebró una conferencia de prensa en el 25º período de sesiones del Consejo de Derechos Humanos.

III. La lucha contra el terrorismo y la vigilancia digital a gran escala

A. Introducción y sinopsis

6. El crecimiento exponencial de las capacidades tecnológicas de los Estados en el último decenio ha mejorado la capacidad de los organismos de inteligencia y encargados de hacer cumplir la ley de vigilar selectivamente a personas y organizaciones sospechosas. La intervención de las comunicaciones es una fuente de información valiosa con la que los Estados pueden investigar, prevenir y enjuiciar

actos de terrorismo y otros delitos graves. La mayoría de los Estados son actualmente capaces de intervenir y vigilar las llamadas realizadas con teléfonos fijos o móviles, lo que permite determinar dónde se encuentra una persona, seguir sus movimientos analizando las comunicaciones de telefonía móvil, y leer y grabar sus mensajes de texto. La vigilancia selectiva también permite a los organismos de inteligencia y encargados de hacer cumplir la ley vigilar la actividad en línea de personas específicas, ingresar en bases de datos y dispositivos de computación en la nube, y obtener la información almacenada en ellos. Un número creciente de Estados utiliza sistemas de software maligno que pueden servir para infiltrarse en la computadora o el teléfono inteligente de una persona, modificar su configuración y vigilar su actividad. En conjunto, estas formas de vigilancia proporcionan un mosaico de datos de fuentes múltiples que puede generar información valiosa sobre una persona u organización en particular.

7. La característica común de estas técnicas de vigilancia es que dependen de que se sospeche previamente de la persona o la organización que se someterá a vigilancia. En esos casos, los Estados casi invariablemente exigen algún tipo de autorización previa (ya sea del poder judicial o ejecutivo), y en algunos de ellos existe un nivel adicional de examen independiente *a posteriori*. En la mayoría de los Estados, por lo tanto, hay al menos una oportunidad (y a veces más de una) de examinar la información que supuestamente generó sospechas, y de evaluar la legalidad y la proporcionalidad de las medidas de vigilancia tomadas en función de los hechos del caso en particular. Con la vigilancia selectiva, se puede evaluar objetivamente la necesidad y la proporcionalidad de la vigilancia prevista, comparando el grado de intrusión propuesto con la utilidad que esta tendría para una investigación concreta.

8. Sin embargo, la velocidad con la que cambia la tecnología ha permitido que algunos Estados accedan de manera masiva a los datos de tráfico y de contenido de las comunicaciones sin que exista una sospecha previa. Las autoridades competentes de estos Estados ahora pueden aplicar algoritmos de extracción automatizada de datos (“data mining”) para captar un universo potencialmente ilimitado de tráfico de comunicaciones. Al intervenir los cables de fibra óptica por los que se transmite la mayoría de las comunicaciones digitales, los Estados en cuestión han podido vigilar a gran escala los metadatos y el contenido de las comunicaciones, lo cual les ha dado a los organismos de inteligencia y encargados de hacer cumplir la ley la posibilidad de vigilar y grabar no solo las comunicaciones de sus propios ciudadanos, sino también las de personas que se encuentran en otros Estados. Esta capacidad suele verse reforzada por las leyes de conservación obligatoria de datos que obligan a los proveedores de servicios de telecomunicaciones e Internet a conservar los datos de tráfico de las comunicaciones para su inspección y análisis. Utilizando software de escaneo, criterios para la definición de perfiles y términos de búsqueda específicos, las autoridades competentes pueden filtrar grandes cantidades de información almacenada para detectar patrones de comunicación entre las personas y las organizaciones. Los algoritmos de extracción automatizada de datos vinculan nombres, lugares, números y direcciones de protocolo de Internet comunes e identificativos, y buscan correlaciones, intersecciones geográficas de los datos de ubicación y patrones de las relaciones en línea, ya sean sociales o de otro tipo[1].

[1] http://blog.privacystrategy.eu/public/published/Submission_ISC_7.2.2014_-_Caspar_Bowden.pdf.

9. De este modo, los Estados con altos niveles de penetración de Internet pueden tener acceso al contenido telefónico o de correo electrónico de un número realmente ilimitado de usuarios, y tener una visión general de las actividades de Internet relacionadas con determinados sitios web. Todo esto es posible sin que existan sospechas previas respecto de una persona u organización específicas. Las comunicaciones de literalmente todos los usuarios de Internet pueden ser inspeccionadas por los organismos de inteligencia y encargados de hacer cumplir la ley en estos Estados. Esta práctica equivale a una injerencia sistemática en el derecho al respeto de la privacidad de las comunicaciones y, en consecuencia, requiere una justificación convincente.

10. Desde el punto de vista de la aplicación de la ley, el valor añadido de la tecnología de vigilancia a gran escala se deriva justamente del hecho de que permite vigilar las comunicaciones de las personas y las organizaciones en las que las autoridades no habían reparado. Se sostiene que el beneficio para el interés público que ofrece la tecnología de acceso masivo se deriva precisamente de que no se necesita una sospecha previa. Este razonamiento circular solo puede conciliarse sometiendo la práctica de los Estados en esta esfera al análisis previsto en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos.

11. El artículo 17 del Pacto establece que toda injerencia en las comunicaciones privadas debe estar autorizada por ley, y debe ser un medio necesario y proporcionado para alcanzar un objetivo legítimo de una política pública (véanse los párrs. 28 a 31). Si bien no cabe duda de que la prevención del terrorismo es un objetivo legítimo de esta injerencia (véanse los párrs. 33 y 34), las actividades de los organismos de inteligencia y encargados de hacer cumplir la ley en este ámbito deben igualmente respetar el derecho internacional de los derechos humanos[2]. Limitarse a afirmar, sin hacer precisiones, que la tecnología de vigilancia a gran escala puede contribuir a la represión y el enjuiciamiento de los actos de terrorismo no es justificación suficiente para su uso en el ámbito del derecho de los derechos humanos. Que algo sea técnicamente factible, y que a veces pueda proporcionar información útil, no significa que sea en sí mismo razonable o legal (en términos del derecho internacional o nacional) (véase A/HRC/27/37, párr. 24).

12. El derecho internacional de los derechos humanos exige que los Estados justifiquen con claridad y pruebas cualquier injerencia en el derecho a la privacidad, ya sea individual o a gran escala. Es axioma central de la proporcionalidad que cuanto mayor sea la injerencia en los derechos humanos protegidos, más convincente deberá ser la justificación para satisfacer los requisitos del Pacto. La dura realidad es que el uso de la tecnología de vigilancia a gran escala realmente suprime por completo el derecho a la privacidad de las comunicaciones en Internet. Al posibilitar el acceso masivo a todo el tráfico de las comunicaciones digitales, esta tecnología impide realizar un análisis individualizado de proporcionalidad. Además, permite interferir en las comunicaciones privadas sin autorización independiente o previa, o de cualquier otro tipo, sobre la base de la sospecha que se tiene de una persona u organización en particular. El análisis previo, por lo tanto, solo es posible al nivel de generalidad más alto.

[2] Véase la recopilación de buenas prácticas relacionadas con los marcos y las medidas de carácter jurídico e institucional aplicables a los servicios de inteligencia y su supervisión, elaboradas por el anterior Relator Especial (A/HRC/14/46, párrs. 9 a 50).

13. Dado que no existe una justificación relativa a un caso concreto para tomar medidas de vigilancia a gran escala, es responsabilidad de los Estados pertinentes justificar la práctica general de acceder de manera masiva a las comunicaciones digitales. De este modo, el análisis de proporcionalidad pasa del nivel particular (evaluar la justificación para invadir la privacidad de una persona o una organización determinada) al nivel general (evaluar la justificación para adoptar un sistema que supone la injerencia indiscriminada en los derechos a la privacidad individuales y colectivos de todos los usuarios de Internet). La magnitud de la injerencia en los derechos a la privacidad es tal que se requiere una justificación de política pública de igual magnitud.

14. El artículo 17 dispone que, como mínimo, los Estados que utilizan tecnología de vigilancia a gran escala den cuenta pública y coherentemente de los beneficios tangibles que se derivan de su uso. Sin esa justificación, sencillamente no se puede evaluar la compatibilidad de esta nueva práctica de los Estados con los requisitos del Pacto. La evaluación de la proporcionalidad en este contexto consiste en encontrar el equilibrio entre, por una parte, el interés de la sociedad en proteger la privacidad en línea, y, por la otra, los imperativos indiscutibles de la lucha eficaz contra el terrorismo y de la aplicación de la ley. Para determinar dónde se encuentra ese equilibrio es preciso que se celebre un debate público y fundamentado dentro de los Estados y entre ellos. Es necesario que la comunidad internacional confronte de lleno esta revolución en nuestra concepción colectiva de la relación entre las personas y el Estado[3]. Para poder evaluar la legalidad de estas medidas es preciso, primeramente, que los Estados que usan esta tecnología sean claros respecto a su metodología y su justificación[4]. De lo contrario, se corre el riesgo de que la injerencia sistemática en la seguridad de las comunicaciones digitales siga proliferando sin que se analicen detenidamente las consecuencias del abandono general del derecho a la privacidad en línea. Si los Estados que usan esta tecnología monopolizan la información sobre sus consecuencias, imperará una forma de censura conceptual que impedirá que se mantenga un debate fundamentado.

15. Hay quienes afirman que, para empezar, los usuarios de Internet no pueden razonablemente creer que tendrán privacidad, y deben asumir que sus comunicaciones pueden ser vigiladas tanto por entidades privadas como estatales. La clásica analogía que trazan quienes apoyan esta opinión es la que equipara el envío de un correo electrónico sin encriptar con el envío de una postal. Independientemente de sus méritos, esta comparación no responde a las cuestiones fundamentales de legalidad, necesidad y proporcionalidad. La finalidad misma del requisito del Pacto que exige que la injerencia del Estado en las comunicaciones esté regida por legislación expresa y accesible públicamente es que las personas puedan saber cuál es el alcance de los derechos a la privacidad de los que efectivamente gozan y prever las circunstancias en que sus comunicaciones podrían

[3] Como señaló la Junta de Supervisión de la Privacidad y las Libertades Civiles: “Permitir que el Gobierno recopile rutinariamente los registros de llamadas de todo el país genera un profundo desequilibrio en la relación de poder que existe entre el Estado y los ciudadanos”; Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court”.

[4] En su informe sobre el derecho a la privacidad en la era digital (A/HRC/27/37, párr. 48), la Alta Comisionada para los Derechos Humanos observó “la preocupante falta de transparencia gubernamental asociada a las políticas, leyes y prácticas de vigilancia, que dificulta todo intento de evaluar su compatibilidad con el derecho internacional de los derechos humanos y asegurar la rendición de cuentas”.

ser vigiladas (véanse los párrs. 35 a 39). No obstante, el valor de esta tecnología como herramienta de lucha contra el terrorismo y para la aplicación de la ley reside en la suposición de los usuarios de Internet de que sus comunicaciones son confidenciales (de lo contrario, no tendría ningún objeto interferirlas). Esto se refleja en las declaraciones efectuadas por miembros de los servicios de inteligencia de los Estados Unidos de América y el Reino Unido de Gran Bretaña e Irlanda del Norte tras darse a conocer que ambos Estados mantenían programas de vigilancia a gran escala, según las cuales revelar la existencia de estos programas había causado un daño en la seguridad nacional pues de esta forma se había alertado a posibles terroristas de que sus comunicaciones estaban siendo vigiladas[5].

16. Toda evaluación de la proporcionalidad debe también tener plenamente en cuenta que Internet es ahora un medio de comunicación omnipresente para varios millones de personas en todo el mundo. La revolución en el ámbito de la tecnología digital ha cambiado enormemente la forma en que nos comunicamos. Las tecnologías de comunicación digitales que utilizan Internet (incluidos los aparatos portátiles y los teléfonos inteligentes) han pasado a formar parte de nuestra vida cotidiana (véase A/HRC/27/37, párr. 1). Hoy en día, quienes deseen participar en el intercambio de información e ideas en el mundo moderno de las comunicaciones mundiales se ven obligados a utilizar tecnologías de comunicación digitales y transnacionales. El tráfico de Internet a menudo se distribuye a través de servidores ubicados en jurisdicciones extranjeras. La idea de que los usuarios han renunciado voluntariamente a su derecho a la privacidad es totalmente infundada (*ibid*., párr. 18). Existe un principio general del derecho internacional de los derechos humanos según el cual puede interpretarse que una persona ha renunciado a un derecho humano protegido únicamente cuando renuncia a él expresa, inequívoca y voluntariamente con conocimiento de causa. En el mundo digital moderno, el mero hecho de utilizar Internet como medio de comunicación privada no puede de ninguna manera constituir una renuncia con conocimiento de causa al derecho a la privacidad consagrado en el artículo 17 del Pacto.

17. Internet no es un espacio estrictamente público y está formado por numerosas capas de esferas privadas, sociales y públicas[1]. Quienes utilizan a sabiendas plataformas de las redes sociales en las que se publican mensajes a la vista de todos, obviamente no pueden tener una expectativa razonable de privacidad. La analogía de las postales es completamente válida para la difusión de información a través de ámbitos públicos, como, por ejemplo, Twitter y Facebook, o de mensajes publicados en sitios web públicos. Pero leer una postal no es una analogía válida para la intervención de mensajes privados enviados por correo electrónico, estén o no encriptados.

18. Suponiendo, por consiguiente, que sigue existiendo un derecho al respeto de la privacidad de las comunicaciones digitales (y esto no puede negarse (véase la resolución 68/167 de la Asamblea General)), la adopción de tecnología de vigilancia a gran escala sin duda menoscaba la esencia misma de ese derecho (véanse los párrs. 51 y 52). Su uso es potencialmente incompatible con el principio básico de que los Estados adopten los medios menos perturbadores disponibles cuando invaden los derechos humanos protegidos (véase el párr. 51), excluye cualquier evaluación

[5] Véase http://abcnews.go.com/Blotter/intel-heads-edward-snowden-profound-damage-us-security/story?id=22285388; y www.itv.com/news/2013-10-09/the-damage-of-edward-snowdens-revelations/.

individualizada de la proporcionalidad (véase el párr. 52), y está rodeado de argumentos de confidencialidad que dificultan enormemente cualquier otro tipo de análisis de proporcionalidad (véanse los párrs. 51 y 52). Los Estados que realizan vigilancia a gran escala hasta ahora no han conseguido justificar públicamente su necesidad en detalle y con pruebas, y casi ningún Estado ha promulgado legislación nacional que autorice expresamente su uso (véase el párr. 37). Desde el punto de vista del artículo 17 del Pacto, esto prácticamente equivale a derogar por completo el derecho a la privacidad de las comunicaciones digitales. Por estos motivos, la vigilancia a gran escala de los datos de tráfico y de contenido de las comunicaciones digitales es una gran amenaza para una norma establecida del derecho internacional. En opinión del Relator Especial, la existencia misma de programas de vigilancia a gran escala constituye una injerencia potencialmente desproporcionada en el derecho a la privacidad[6]. En pocas palabras, que los Estados recopilen todas las comunicaciones o los metadatos en todo momento de manera indiscriminada es incompatible con las concepciones de la privacidad vigentes. La esencia misma del derecho a la privacidad de las comunicaciones es que solo se lo puede vulnerar excepcionalmente, justificando la injerencia en cada caso en particular (véase el párr. 51).

19. Aunque es posible que en la lucha contra el terrorismo exista una justificación convincente para la revaluación radical de los derechos a la privacidad en Internet que requieren estas prácticas, los argumentos a favor de derogar por completo el derecho a la privacidad en Internet no han sido presentados públicamente por los Estados interesados ni sometidos a escrutinio y debate. La amenaza del terrorismo puede justificar la vigilancia a gran escala únicamente si los Estados que utilizan esta tecnología pueden demostrar pormenorizadamente las ventajas tangibles que genera para la lucha contra el terrorismo. Además, las medidas justificadas en función del deber de los Estados de proporcionar protección contra la amenaza del terrorismo nunca deberían utilizarse como caballo de Troya para ampliar las facultades de vigilancia en funciones gubernamentales inconexas. Existe un riesgo permanente de que se produzca una "expansión de la finalidad", en la cual las medidas justificadas por la lucha contra el terrorismo se ponen a disposición de autoridades públicas para fines de mucho menor interés público (véase el párr. 55). En el presente informe, el Relator Especial toma como base la labor de su predecesor (A/HRC/13/37) y del anterior Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión (A/HRC/23/40). El Relator sostiene que los Estados que utilizan tecnología de vigilancia de acceso masivo tienen el deber de explicar rápida, precisa y públicamente por qué se justifica esta intrusión indiscriminada en la privacidad colectiva para prevenir el terrorismo u otros delitos graves.

B. Revelaciones recientes sobre la naturaleza y el alcance de las capacidades de vigilancia digital de los Estados

20. El 5 de junio de 2013, un periódico nacional del Reino Unido publicó el contenido de una orden judicial clasificada dictada por el Tribunal de Vigilancia de Inteligencia Extranjera de los Estados Unidos en virtud del artículo 215 de la Ley

[6] Véase también la opinión de la Alta Comisionada para los Derechos Humanos, A/HRC/27/37, párrs. 20 y 25.

USA PATRIOT. La orden judicial supuestamente obligaba a uno de los mayores proveedores de telecomunicaciones de los Estados Unidos a entregar diariamente al Organismo Nacional de Seguridad todos los "metadatos telefónicos" por un período de tres meses y prohibía a la empresa que revelara la existencia de la solicitud o de la propia orden judicial. El 6 de junio de 2013, un periódico de los Estados Unidos publicó otro artículo en el que reveló la existencia de un programa digital secreto del Organismo Nacional de Seguridad denominado PRISM. El programa, supuestamente autorizado por el artículo 702 de la Ley de Vigilancia de Inteligencia Extranjera de los Estados Unidos, al parecer recababa datos de contenido de los servidores centrales de nueve de las principales empresas tecnológicas de los Estados Unidos.

21. Según los informes publicados en ambos periódicos, el material recopilado a través del programa PRISM se puso a disposición de otros organismos de inteligencia, entre ellos el Centro Gubernamental de Comunicaciones del Reino Unido. La información divulgada posteriormente reveló la existencia de otro programa de recopilación de datos denominado Upstream, en el que supuestamente se captaban las comunicaciones telefónicas y de Internet transmitidas por cables de fibra óptica e infraestructura de propiedad de proveedores de servicios estadounidenses. Gran parte del tráfico de Internet de todo el mundo se transmite a través de servidores ubicados físicamente en los Estados Unidos.

22. Los medios de comunicación informaron seguidamente de que la Dirección de Inteligencia de Sistemas del Organismo Nacional de Seguridad dispone de una subdivisión de vulnerabilidades en las aplicaciones que recopila datos de los sistemas de comunicaciones de todo el mundo. Al parecer el Organismo opera un mecanismo de explotación de Internet denominado Quantum, que le permite ingresar en las computadoras de terceros. Según se informa, esta metodología implica tomar secretamente el control (o "apoderarse") de los servidores en lugares clave del "pilar" de Internet. El programa Quantum se hace pasar por determinados sitios web (incluidos sitios comunes como la página de búsqueda de Google) para introducir un programa de control a distancia no autorizado en las computadoras y los dispositivos con Wi-Fi de las personas que visitan el sitio falso (quienes, por supuesto, no tienen ningún motivo para dudar de su autenticidad). Los expertos en tecnología consideran que esta metodología puede exponer a las computadoras de los usuarios a una vulnerabilidad permanente, lo cual garantiza que se siga transmitiendo información al Organismo Nacional de Seguridad de los Estados Unidos indefinidamente.

23. Los poderes ejecutivo y legislativo de los Estados Unidos posteriormente tomaron una serie de medidas en respuesta a estas revelaciones. Una cuestión que se ha observado en este proceso es la diferencia de trato entre los ciudadanos de los Estados Unidos y quienes no lo son (incluso quienes se encuentran en la jurisdicción territorial de los Estados Unidos de América). Los principales hechos se resumen a continuación:

a) El 9 de agosto de 2013, el Presidente Barack Obama anunció que había solicitado a la Junta de Supervisión de la Privacidad y las Libertades Civiles[7] que examinara las medidas contra el terrorismo que se encontraban vigentes en ese

[7] La Junta es un organismo independiente del poder ejecutivo facultado para examinar y analizar las operaciones de lucha contra el terrorismo y para velar por que guarden una relación equilibrada con la necesidad de proteger la privacidad y las libertades civiles; véase www.pclob.gov/.

momento[8]. A fines de agosto de 2013, la Junta pidió al Director del Servicio Nacional de Inteligencia y al Fiscal General que actualizara los procedimientos que utilizaban los servicios de inteligencia para recopilar, conservar y difundir información relacionada con los ciudadanos de los Estados Unidos[9];

b) El 12 de diciembre de 2013, el Grupo de Examen del Presidente presentó su informe titulado “Liberty and security in a changing world”, en el que formuló una serie de recomendaciones importantes de reforma. En respuesta a ese informe, el 17 de enero de 2014, el Presidente Obama anunció una serie de propuestas de cambios legislativos y administrativos[10]. Al mismo tiempo, el Gobierno publicó una nueva Directriz Normativa Presidencial, “PPD-28”, para reforzar la supervisión de las actividades de inteligencia de señales de los servicios de inteligencia, tanto dentro como fuera de los Estados Unidos[11];

c) El 23 de enero de 2014, la Junta de Supervisión de la Privacidad y las Libertades Civiles publicó el primero de dos informes en los que la mayoría llegó a la conclusión de que el programa de metadatos telefónicos era incompatible con la legislación nacional porque el artículo 215 de la Ley USA PATRIOT no ofrecía fundamento suficiente para su uso[12]. El 27 de marzo, el Presidente Obama anunció una nueva serie de propuestas para poner fin al programa[13]. El 22 de mayo de 2014, la Cámara de Representantes aprobó la Ley de Libertad de los Estados Unidos, que incorporó algunas de las propuestas del Presidente;

d) El 2 de julio de 2014, la Junta de Supervisión de la Privacidad y las Libertades Civiles publicó un segundo informe en el que se detallaba el funcionamiento en la práctica de las operaciones de vigilancia realizadas con arreglo al artículo 702 de la Ley de Vigilancia de Inteligencia Extranjera[14]. Si bien la principal preocupación expresada en el informe era la compatibilidad de estos programas con los requisitos constitucionales y legislativos de los Estados Unidos, la Junta reconoció que también planteaban “interrogantes normativos y legales importantes pero difíciles” respecto al tratamiento de los extranjeros[15]. La Junta consideró que la aplicación del derecho a la privacidad en la vigilancia de seguridad nacional realizada en un país que podía afectar a los residentes de otro país no era una cuestión “zanjada” entre los Estados partes en el Pacto Internacional de Derechos Civiles y Políticos, una hipótesis que en su opinión quedaba demostrada por el “debate intenso” que estaba teniendo lugar[16].

---

[8] Véase www.whitehouse.gov/the-press-office/2013/08/09/remarks-president-press-conference.

[9] Véase www.pclob.gov/newsroom.

[10] Véase www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcbd84_story.html.

[11] Véase www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence.

[12] “Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court”.

[13] Véase www.whitehouse.gov/the-press-office/2014/03/27/fact-sheet-administration-s-proposal-ending-section-215-bulk-telephony-m.

[14] “Report on the Surveillance Program Operated Pursuant to Section 702 of the FISA”, véase www.pclob.gov/meetings-and-events/2014meetingsevents/02-july-2014-public-meeting.

[15] *Ibid*., pág. 98.

[16] *Ibid*., pág. 100.

24. En el Reino Unido ha tenido lugar un proceso de examen paralelo. El 10 de junio de 2013, en respuesta a las denuncias de que el Centro Gubernamental de Comunicaciones había eludido la legislación del Reino Unido al utilizar el programa PRISM del Organismo Nacional de Seguridad para acceder al contenido de las comunicaciones a las que no se podía acceder con arreglo a la legislación nacional, el Secretario de Relaciones Exteriores declaró ante el Parlamento que los datos proporcionados por los Estados Unidos sobre ciudadanos del Reino Unido estaban "sujetos a los controles y las salvaguardas legislativas correspondientes del Reino Unido", incluidas las disposiciones pertinentes de la Ley de Servicios de Inteligencia de 1994, la Ley de Derechos Humanos de 1998 y la Ley de Reglamentación de las Facultades de Investigación de 2000[17].

25. El 21 de junio de 2013, los medios de comunicación informaron de la existencia de otro programa que llevaba adelante el Centro Gubernamental de Comunicaciones ("Tempora"), en el cual al parecer se colocaban dispositivos de intervención de datos en los cables de fibra óptica que unían el Reino Unido y los Estados Unidos para facilitar la intervención de la información de contenidos y metadatos. Tanto dentro como fuera del Parlamento del Reino Unido se ha puesto en duda que la legislación vigente confiera al Centro Gubernamental de Comunicaciones facultades que le permitan realizar este tipo de operaciones y que estas respeten el derecho a la privacidad garantizado en el artículo 8 del Convenio Europeo de Derechos Humanos[18]. La información revelada posteriormente tuvo que ver principalmente con la función del Grupo Conjunto de Inteligencia sobre Amenazas del Centro Gubernamental de Comunicaciones. Según se informa, este organismo introdujo un virus informático llamado "Recepción del Embajador" para realizar actividades encubiertas en línea. Al parecer el virus puede autoencriptarse y comportarse como un "camaleón", imitando las comunicaciones de otros usuarios de Internet.

26. Tras una investigación preliminar del acceso del Centro Gubernamental de Comunicaciones a los datos de tráfico y de contenido de las comunicaciones, el Comité de Inteligencia y Seguridad (comité parlamentario encargado de supervisar los servicios de inteligencia)[19] emitió un comunicado el 17 de julio de 2013. Luego de analizar el marco jurídico que regía los acuerdos de intercambio de información entre el Centro Gubernamental de Comunicaciones y sus homólogos extranjeros, el Comité llegó a la conclusión de que no se había violado ninguna ley del Reino Unido y que el Centro había procedido con arreglo a las obligaciones legales que le incumbían en virtud de la Ley de Servicios de Inteligencia de 1994. No obstante, el Comité llegó a la conclusión de que era necesario seguir investigando para determinar si el marco legislativo vigente que regulaba el acceso a las comunicaciones privadas era adecuado dada la "compleja interacción" que existía entre la Ley de Servicios de Inteligencia de 1994, la Ley de Derechos Humanos de 1998 y la Ley de Reglamentación de las Facultades de Investigación de 2000. El 17 de octubre de 2013, el Comité de Inteligencia y Seguridad anunció que ampliaría su investigación a raíz de la preocupación en torno al alcance de las capacidades de los servicios de inteligencia y al efecto de sus operaciones en el derecho a la privacidad[20].

---

[17] Véase www.gov.uk/government/speeches/foreign-secretary-statement-to-the-house-of-commons-gchq.

[18] Véase www.theguardian.com/uk-news/2013/oct/14/conservative-peer-spying-gchq-surveillance; y www.publications.parliament.uk/pa/cm201314/cmhansrd/cm131031/halltext/131031h0001.htm.

[19] Véase http://isc.independent.gov.uk/.

[20] Véase http://isc.independent.gov.uk/news-archive/17october2013.

27. El 8 de abril de 2014, el Tribunal de Justicia de la Unión Europea dio a conocer la sentencia dictada en el asunto *Digital Rights Ireland*, en la que afirmó que la Directiva de la Unión Europea sobre la Conservación de Datos era incompatible con el derecho al respeto de la vida privada y el derecho a la protección de los datos de carácter personal, ambos garantizados en la Carta de los Derechos Fundamentales de la Unión Europea[21]. La Directiva obligaba a los proveedores de servicios de comunicaciones a conservar los datos de tráfico para que las autoridades nacionales competentes pudieran acceder a ellos a fin de prevenir, investigar, detectar y enjuiciar delitos graves, incluido el terrorismo. Al afirmar que la conservación de los datos de tráfico y el acceso a ellos constituían una "injerencia especialmente grave" en ambos derechos, el Tribunal de Justicia de la Unión Europea determinó que la Directiva no satisfacía el principio de proporcionalidad. El 10 de julio de 2014, el Gobierno del Reino Unido presentó el Proyecto de Ley de Facultades de Investigación y Conservación de Datos en respuesta a la decisión del Tribunal. El Gobierno sostuvo que el proyecto (que ahora es ley) era una medida para "aclarar" la naturaleza y el alcance de las obligaciones que podían imponerse a los proveedores de servicios de telecomunicaciones e Internet con sede en el Reino Unido[22].

C. La vigilancia a gran escala, la lucha contra el terrorismo y el derecho a la privacidad

1. El derecho a la privacidad en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos

28. La privacidad puede definirse como la presunción de que el individuo debe tener una esfera de desarrollo autónomo personal, interacción y libertad, libre de la intervención del Estado y de la intrusión excesiva no solicitada de otros individuos no invitados (véase A/HRC/23/40, párr. 22; y A/HRC/13/37, párr. 11). El deber de respetar la privacidad y la seguridad de las comunicaciones implica que las personas tienen derecho a compartir información e ideas entre sí sin la injerencia del Estado (o de un agente privado), con la certeza de que sus comunicaciones llegarán a sus destinatarios y solo estos las leerán[23]. El derecho a la privacidad también incluye el derecho de las personas a saber quién posee información sobre ellas y cómo se utiliza[24].

29. El artículo 17 del Pacto Internacional de Derechos Civiles y Políticos es la disposición jurídicamente vinculante más importante incluida en un tratado que garantice el derecho a la privacidad a nivel universal. Establece que "nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación" y que "toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques". Existen otros instrumentos de derechos humanos que contienen disposiciones similares y leyes regionales y nacionales que también reflejan el derecho de todas las personas al respeto de su vida privada y familiar, su domicilio y su correspondencia.

---

[21] Tribunal de Justicia de la Unión Europea, sentencia de 8 de abril de 2014 en los asuntos acumulados C-293/12 y C-594/12, *Digital Rights Ireland Ltd y Seitlinger y otros*.

[22] Véase www.gov.uk/government/speeches/communications-data-and-interception.

[23] Observación general núm. 16 del Comité de Derechos Humanos, párr. 8.

[24] *Ibid*., párr. 10; véase A/HRC/23/40, párr. 22.

30. No obstante, el derecho a la privacidad no es un derecho absoluto. Una vez que se sospecha de una persona y que los organismos de inteligencia y encargados de hacer cumplir la ley la investigan oficialmente, se la puede vigilar con fines completamente legítimos en el marco de la lucha contra el terrorismo y de la aplicación de la ley (véase A/HRC/13/37, párr. 13). Aunque el artículo 17 del Pacto no contiene una cláusula específica de limitación que describa las circunstancias en que la injerencia en el derecho a la privacidad podría ser compatible con el Pacto, se interpreta unánimemente que permite que se adopten este tipo de medidas siempre que a) estén autorizadas por una ley nacional que sea accesible y precisa y que se ajuste a los requisitos del Pacto[25], b) tengan un objetivo legítimo, y c) cumplan los criterios de necesidad y proporcionalidad[26].

31. Cuando se reparó en que una gran parte del tráfico mundial de Internet pasaba en algún momento por los Estados Unidos, varios Estados se mostraron preocupados por la posibilidad de que el derecho a la privacidad de sus ciudadanos hubiera sido vulnerado por el programa PRISM. En diciembre de 2013, la Asamblea General aprobó la resolución 68/167 sobre el derecho a la privacidad en la era digital, copatrocinada por 57 Estados Miembros y aprobada sin someterla a votación. En esa resolución, la Asamblea afirmó que el derecho a la privacidad debía estar protegido en Internet y exhortó a los Estados a que examinaran sus procedimientos, prácticas y legislación relativos a la vigilancia y la interceptación de las comunicaciones y la recopilación de datos personales, haciendo hincapié en la necesidad de que los Estados velaran por que se diera cumplimiento pleno y efectivo de todas sus obligaciones en virtud del derecho internacional de los derechos humanos.

32. En la misma resolución, la Asamblea General también encomendó a la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos que presentara al Consejo de Derechos Humanos y a la Asamblea General un informe sobre la protección y la promoción del derecho a la privacidad en el contexto de la vigilancia y la interceptación de las comunicaciones digitales y la recopilación de datos personales en los planos nacional y extraterritorial, incluso a gran escala. En el párrafo 47 de su informe, publicado el 30 de junio de 2014 (A/HRC/27/37), la Alta Comisionada llegó a la conclusión de que el derecho internacional de los derechos humanos proporcionaba un marco claro y universal para la promoción y la protección del derecho a la privacidad, también en el contexto de la vigilancia nacional y extraterritorial, la interceptación de las comunicaciones digitales y la recopilación de datos personales. No obstante, señaló que las prácticas en muchos Estados habían puesto de manifiesto una carencia de leyes nacionales adecuadas y/o de aplicación de las mismas, insuficientes garantías procesales y capacidades de supervisión ineficaces, elementos que habían contribuido a la falta de rendición de cuentas por las injerencias arbitrarias o ilegales en el derecho a la privacidad. La Alta Comisionada destacó que seguía saliendo a la luz información sobre la naturaleza y el alcance de las operaciones de vigilancia digital,

[25] Observación general núm. 16 del Comité de Derechos Humanos, párr. 3.

[26] Véase A/HRC/27/37, párrs. 22 a 25 y las fuentes allí citadas; A/HRC/23/40, párrs. 28 y 29; A/HRC/13/37, párrs. 13 a 17; Principios de Siracusa sobre las disposiciones de limitación y derogación del Pacto Internacional de Derechos Civiles y Políticos, E/CN.4/1985/4, anexo; Observaciones generales núms. 16, 27, 29, 34 y 31 del Comité de Derechos Humanos; Comité de Derechos Humanos, *Van Hulst c. los Países Bajos*, Comunicación núm. 903/2999, 2004; *Madafferi c. Australia*, Comunicación núm. 1011/2001, 2004; *Toonen c. Australia*, Comunicación núm. 488/1992, párr. 8.3; *MG c. Alemania*, Comunicación núm. 1482/2006, 2008; y CCPR/C/USA/CO/4.

pero expresó su inquietud por “la preocupante falta de transparencia gubernamental asociada a las políticas, leyes y prácticas de vigilancia, que dificulta todo intento de evaluar su compatibilidad con el derecho internacional de los derechos humanos y asegurar la rendición de cuentas” (*ibid*., párr. 48). Por otra parte, pidió a los Estados que revisaran sus leyes y práctica nacionales para garantizar su conformidad con las normas internacionales de derechos humanos, y que realizaran las modificaciones necesarias. Además, pidió a la comunidad internacional que realizara un análisis en profundidad de estas cuestiones (*ibid*., párrs. 49 y 51).

2. La lucha contra el terrorismo como objetivo legítimo

33. A diferencia de algunos derechos condicionados protegidos por el Pacto, el artículo 17 no realiza una enumeración exhaustiva de objetivos legítimos de política pública que podrían justificar una injerencia en el derecho a la privacidad. Sin embargo, la prevención, la represión y la investigación de los actos de terrorismo constituyen claramente un objetivo legítimo a los efectos del artículo 17. El terrorismo puede desestabilizar las comunidades, amenazar el desarrollo social y económico, fracturar la integridad territorial de los Estados, y socavar la paz y la seguridad internacionales. Según lo dispuesto en el artículo 6 del Pacto, los Estados tienen la obligación positiva de proteger contra actos de terrorismo a los ciudadanos y las personas que se encuentren dentro de su jurisdicción. Un aspecto de esta obligación es el deber de establecer mecanismos eficaces para detectar posibles amenazas terroristas antes de que se materialicen. Los Estados cumplen con este deber cuando los organismos de inteligencia y encargados de hacer cumplir la ley reúnen y analizan la información pertinente (véase A/HRC/20/14, párr. 21).

34. La mayor capacidad de los Estados de vigilar todo el tráfico de Internet es, según se afirma, de particular importancia en el contexto de la lucha contra el terrorismo porque las comunicaciones por Internet han sido un elemento importante en la financiación y comisión de actos de terrorismo internacional; porque las organizaciones terroristas han utilizado Internet para reclutar miembros; y porque, de lo contrario, la identificación anticipada de las personas involucradas en la planificación o la instigación de actos de terrorismo podría verse obstaculizada por las limitaciones de inteligencia. Puesto que el terrorismo es una actividad mundial, la búsqueda de quienes están implicados en él debe trascender las fronteras nacionales. La prevención y represión del terrorismo es, por lo tanto, un imperativo de interés público que reviste la mayor importancia y podría ser, en principio, una justificación plausible de la vigilancia de Internet a gran escala.

3. La vigilancia a gran escala y el requisito de la calidad de la ley

35. El artículo 17 del Pacto establece expresamente que toda persona tiene derecho a la protección de la ley contra las injerencias arbitrarias o ilegales en su vida privada. Esto implica un requisito de “calidad de la ley” que impone tres condiciones: a) la medida debe encontrar cierto fundamento en una ley nacional; b) la propia ley nacional debe ser compatible con el estado de derecho y los requisitos del Pacto; y c) las disposiciones pertinentes de la ley nacional deben ser accesibles, claras y precisas. Una injerencia autorizada por una ley nacional puede, no obstante, ser “ilegal” y “arbitraria” a los efectos del artículo 17 si la legislación nacional pertinente no satisface los requisitos básicos de accesibilidad, especificidad y previsibilidad[27], o si por algún otro

[27] Observación general núm. 16 del Comité de Derechos Humanos, párr. 3.

motivo no se ajusta a los criterios de necesidad y proporcionalidad[28]. En consecuencia, la legislación nacional debe contener disposiciones que aseguren que las facultades de vigilancia intrusiva se ajusten a objetivos legítimos específicos (véase A/HRC/13/37, párr. 60; y A/HRC/27/37, párr. 28), y proporcionar salvaguardas eficaces contra su uso excesivo[29]. Además, se debe circunscribir el ejercicio de la discrecionalidad del poder ejecutivo con claridad razonable en la ley aplicable o en directrices publicadas y vinculantes[30].

36. Para que exista accesibilidad no solo es necesario que esta legislación nacional se publique, sino que también alcance un nivel de claridad y precisión suficiente para que quienes se vean afectados por ella regulen su conducta pudiendo prever las circunstancias en las que podría realizarse una vigilancia intrusiva. En el párrafo 8 de su observación general núm. 16 relativa al derecho a la privacidad, el Comité de Derechos Humanos destacó que en la legislación que autorice la injerencia en las comunicaciones privadas "se deben especificar con detalle las circunstancias precisas en que podrán autorizarse esas injerencias". Antes de la introducción de los programas de vigilancia a gran escala descritos en el presente informe, esta disposición siempre se había interpretado en el sentido de que la legislación nacional debía indicar claramente las condiciones en que podía autorizarse una injerencia y los procedimientos para hacerlo, las categorías de personas cuyas comunicaciones podrían ser intervenidas, el límite de la duración de la vigilancia, y los procedimientos para el uso y el almacenamiento de los datos recopilados[29]. El Tribunal Europeo de Derechos Humanos también ha subrayado la necesidad de contar con normas detalladas y claras sobre la cuestión[31].

37. Los programas de vigilancia a gran escala plantean un problema importante para los requisitos de legalidad previstos en el artículo 17 del Pacto. Cuando se utilizan programas de acceso masivo, no hay límites a las categorías de personas que pueden ser vigiladas ni a la duración de la vigilancia. Estas condiciones, por lo tanto, no pueden enunciarse detalladamente en la legislación. Los marcos jurídicos y administrativos detallados de la vigilancia a gran escala suelen ser confidenciales, y poco se sabe aun públicamente sobre el uso que se da a los datos recabados. Hasta ahora, en muy pocos Estados existe normativa del poder legislativo que autorice expresamente esos programas. En su lugar, se han aplicado a la nueva tecnología digital leyes nacionales desactualizadas concebidas para regular formas de vigilancia más rudimentarias sin modificarlas para reflejar la capacidad mucho mayor que ahora poseen algunos Estados. Se ha sugerido, precisamente, que algunos Estados han "tratado intencionalmente [...] de aplicar sistemas de salvaguardia anticuados y más débiles a informaciones cada vez más sensibles" (véase A/HRC/13/37, párr. 57).

38. El Relator Especial considera que urge que los Estados revisen las leyes nacionales que regulan las formas modernas de vigilancia para asegurarse de que estas prácticas sean compatibles con el derecho internacional de los derechos

[28] *Ibid*., párr. 8.

[29] CCPR/C/USA/CO/4, párr. 22; *Malone v. United Kingdom*, demanda núm. 8691/79, sentencia de 2 de agosto de 1984, párrs. 67 y 68; y *Weber and Saravia v. Germany*, demanda núm. 54934/00, sentencia de 29 de junio de 2006.

[30] A/HRC/27/37, párr. 29; y Principios de Siracusa sobre las disposiciones de limitación y derogación del Pacto Internacional de Derechos Civiles y Políticos (véase E/CN.4/1985/4, anexo), párrs. 16 y 18.

[31] *Weber and Saravia v. Germany*, demanda núm. 54934/00, sentencia de 29 de junio de 2006; *Uzun v. Germany*, EHRR 2012, vol. 54, núm. 121, párr. 35.

humanos. Las leyes nacionales que rigen la intervención de las comunicaciones deberían actualizarse para reflejar formas modernas de vigilancia digital mucho más amplias, y que llegan a niveles mucho más profundos de la vida privada, que las contempladas al promulgarse la mayor parte de la legislación nacional vigente. La falta de legislación clara y actualizada crea un entorno en el que se pueden producir injerencias arbitrarias en el derecho a la privacidad sin que existan salvaguardas acordes. Es fundamental contar con leyes expresas y exhaustivas para garantizar la legalidad y la proporcionalidad en este contexto. Son también un medio indispensable para que las personas puedan prever si sus comunicaciones podrían ser vigiladas y en qué circunstancias.

39. El proceso legislativo público ofrece a los gobiernos la oportunidad de justificar públicamente la aplicación de medidas de vigilancia a gran escala. Los debates públicos permiten que la ciudadanía comprenda el equilibrio que se intenta lograr entre la privacidad y la seguridad (*ibid*., párr. 56). Un proceso de creación de leyes transparente también debería determinar cuáles son las vulnerabilidades inherentes a los sistemas de comunicaciones digitales, para que los usuarios puedan elegir con información. Se trata no solo de un elemento fundamental del requisito de seguridad jurídica contemplado en el artículo 17 del Pacto, sino también de un medio valioso para asegurar la participación efectiva del público en un debate sobre una cuestión de interés público nacional e internacional (véase A/HRC/27/37, párr. 29, y A/HRC/14/46). En opinión del Relator Especial, cuando se interfiere sistemáticamente en los derechos a la privacidad de la comunidad digital en su conjunto, solo una autorización expresa y detallada en una ley promulgada por el poder legislativo permitirá que se verifique el principio de legalidad.

40. Por el contrario, el uso de legislación delegada (instrumentos promulgados por el poder ejecutivo en virtud de facultades delegadas) ya ha permitido que se adopten marcos jurídicos secretos de vigilancia a gran escala, lo cual inhibe la capacidad del poder legislativo, el poder judicial y el público en general de examinar el uso de estas nuevas facultades (véase A/HRC/13/37, párr. 54). Estas disposiciones no satisfacen los requisitos de calidad de la ley previstos en el artículo 17 del Pacto porque no son suficientemente accesibles para el público (véase CCPR/C/USA/CO/4). Si bien puede haber razones legítimas de interés público para mantener la confidencialidad de las especificaciones técnicas y operacionales, estas razones no justifican que no se divulgue al público información genérica sobre la naturaleza y el alcance de la interferencia del Estado en Internet. Sin esa información, es imposible evaluar la legalidad, la necesidad y la proporcionalidad de estas medidas. Por ello, los Estados deberían ser claros con respecto al uso y el alcance de la vigilancia de las comunicaciones a gran escala (véase A/HRC/23/40, párr. 91).

4. Programas de vigilancia extraterritorial a gran escala

41. Algunos Estados tienen la capacidad técnica de vigilar a gran escala las comunicaciones entre personas que no residen en su jurisdicción y, en consecuencia, han implementado prácticas de vigilancia con efectos extraterritoriales. Algunas de estas actividades se llevan a cabo físicamente en el territorio del Estado interesado y, por lo tanto, entran en juego los principios de la jurisdicción territorial contemplados en el Pacto. Esto ocurre no solo cuando los agentes del Estado colocan dispositivos de intervención de datos en los cables de fibra óptica que atraviesan su jurisdicción, sino también cuando los Estados ejercen su autoridad reguladora sobre los proveedores de servicios de telecomunicaciones e Internet que controlan los datos físicamente

(A/HRC/27/37, párr. 34). En ambos casos, la protección de los derechos humanos debe extenderse a las personas cuya privacidad es objeto de injerencia, estén o no físicamente en el país en el que está registrado el proveedor de servicios. Lo mismo cabe decir cuando la legislación de conservación obligatoria de datos impone obligaciones a los proveedores de servicios situados en la jurisdicción territorial o jurídica de un Estado. Incluso cuando los Estados penetran en infraestructuras ubicadas íntegramente fuera de su jurisdicción territorial, las autoridades competentes siguen estando sujetas a las obligaciones que les incumben a los Estados en virtud del Pacto (*ibid*., párrs. 32 a 35 y fuentes allí citadas).

42. Las operaciones de vigilancia extraterritorial plantean dificultades singulares para aplicar el requisito de "calidad de la ley" previsto en el artículo 17 del Pacto. La legislación nacional que rige la intervención de las comunicaciones externas (internacionales) a menudo proporciona menos protección que las disposiciones similares que protegen las comunicaciones estrictamente internas[32]. Preocupa aún más que algunos Estados (entre ellos los Estados Unidos) sigan permitiendo que coexistan regímenes de protección asimétrica para los ciudadanos y los extranjeros. Esta diferencia de trato afecta a todas las comunicaciones digitales, ya que a menudo los mensajes se transmiten a través de servidores ubicados en otras jurisdicciones, y tiene ramificaciones especialmente significativas en la penetración en la computación en la nube[33].

43. Este trato diferenciado en cualquiera de sus dos formas es incompatible con el principio de no discriminación previsto en el artículo 26 del Pacto, principio que también es inherente a la noción misma de proporcionalidad[34]. Además, el uso de programas de vigilancia a gran escala para intervenir las comunicaciones de quienes se encuentran en otras jurisdicciones suscita serios interrogantes sobre la accesibilidad y la previsibilidad de las leyes que rigen la injerencia en el derecho a la privacidad, y sobre la imposibilidad de que las personas sepan que podrían ser objeto de vigilancia extranjera o que sus comunicaciones podrían ser intervenidas en jurisdicciones extranjeras. El Relator Especial considera que los Estados están obligados jurídicamente a proporcionar igual protección a ciudadanos y extranjeros, y a quienes se encuentren dentro y fuera de su jurisdicción.

5. Cooperación internacional entre los organismos de inteligencia

44. Los acuerdos internacionales de intercambio de información de inteligencia suscitan preocupaciones similares. La falta de leyes que regulen los acuerdos de intercambio de información entre los Estados ha dejado el camino abierto a los organismos de inteligencia para celebrar acuerdos bilaterales y multilaterales

[32] En su informe sobre la privacidad en la era digital, la Alta Comisionada señaló varias disposiciones de ese tipo: en los Estados Unidos, la Ley de Vigilancia de Inteligencia Extranjera, art. 1881 a); en el Reino Unido, la Ley de Regulación de las Facultades de Investigación de 2000, art. 8.4; en Nueva Zelandia, la Ley del Servicio de Seguridad del Gobierno de 2003, art. 15A; en Australia, la Ley de Servicios de Inteligencia, art. 9; y en el Canadá, la Ley de Defensa Nacional, art. 273.64, párr. 1 (véase A/HRC/27/37, párr. 35, nota 30).

[33] Dirección General de Políticas Interiores de la Unión del Parlamento Europeo y Casper Bowden, "The US surveillance programmes and their impact on EU citizens' fundamental rights", 2013.

[34] El Comité de Derechos Humanos también destacó la importancia de que se adopten "medidas para que toda interferencia en el derecho a la intimidad se ajuste a los principios de legalidad, proporcionalidad y necesidad, con independencia de la nacionalidad o el emplazamiento de las personas cuyas comunicaciones estén bajo vigilancia directa", CCPR/C/USA/CO/4, párr. 22 a).

clasificados que están fuera del ámbito de supervisión de toda autoridad independiente (véase A/HRC/13/37). La información sobre las comunicaciones individuales puede ser compartida con organismos de inteligencia extranjeros sin la protección de un marco jurídico al que tenga acceso el público y sin salvaguardas adecuadas (o de ningún tipo). Tras un proceso amplio de consultas, la Alta Comisionada para los Derechos Humanos recientemente encontró pruebas fidedignas de que algunos gobiernos habían desviado sistemáticamente la recopilación y el análisis de datos a jurisdicciones con una menor protección de la privacidad (véase A/HRC/27/37, párr. 30). Estas prácticas impiden que los particulares puedan prever el funcionamiento del régimen de vigilancia que los afecta y, por lo tanto, son incompatibles con el artículo 17 del Pacto.

6. Las salvaguardas y la supervisión

45. Una de las principales protecciones que confiere el artículo 17 es la obligación de que los sistemas de vigilancia encubierta cuenten con salvaguardas procesales adecuadas que protejan contra su uso excesivo[29]. Estas salvaguardas pueden adoptar diversas formas, pero generalmente comprenden una autorización independiente previa o una revisión independiente posterior. Las mejores prácticas requieren la participación de los poderes ejecutivo, legislativo y judicial, así como una supervisión civil independiente (véase A/HRC/27/37). La ausencia de salvaguardas adecuadas puede conducir a una falta de rendición de cuentas por las intromisiones arbitrarias o ilegales en el derecho a la privacidad en Internet (*ibid.*).

46. En los lugares donde se llevan adelante programas de vigilancia selectiva, muchos Estados exigen una autorización judicial previa. Si bien la participación del poder judicial con arreglo a las normas internacionales es una salvaguarda importante, se ha comprobado que en algunas jurisdicciones el grado y la efectividad de este escrutinio se ha visto limitado por la deferencia del poder judicial al ejecutivo (*ibid.*, párr. 38). En otros Estados, como el Reino Unido, los ministros de Gobierno libran órdenes de intervención de las comunicaciones con destinatarios específicos sin autorización judicial previa. Estas medidas se justifican con el argumento de que los ministros rinden cuentas democráticamente ante el electorado. El ejercicio de estas facultades por parte del poder ejecutivo es posteriormente examinado por un Comisionado independiente de Intervención de las Comunicaciones, y los particulares también pueden recurrir ante un órgano judicial, el Tribunal de Facultades de Investigación, que está facultado para examinar información clasificada en audiencias celebradas a puerta cerrada.

47. En el contexto de la vigilancia selectiva, independientemente del método de autorización previa que se adopte (del poder judicial o del ejecutivo), hay al menos una oportunidad para examinar previamente la necesidad y proporcionalidad de la medida de vigilancia intrusiva en función de las circunstancias particulares del caso y de la persona u organización cuyas comunicaciones se intervendrán. Ninguna de esas oportunidades se da en el contexto de los programas de vigilancia a gran escala, ya que no dependen de la existencia de sospechas individuales. El examen previo se limita, por tanto, a autorizar la continuación del programa en su conjunto, en lugar de su aplicación a una persona concreta. El Relator Especial considera que los Estados que utilizan tecnología de vigilancia a gran escala deben establecer órganos de supervisión independientes y sólidos que cuenten con recursos suficientes y con el mandato de examinar previamente el uso de técnicas de vigilancia intrusiva para verificar que satisfaga los requisitos de legalidad, necesidad y proporcionalidad contemplados en el artículo 17 del Pacto (A/HRC/13/37, párr. 62).

48. La otra dimensión procesal del artículo 17 es el requisito de realizar un examen *a posteriori* de las medidas de vigilancia intrusiva. Algunos Estados cuentan con un órgano independiente de revisión que supervisa la aplicación de la legislación de vigilancia analizando la forma y el alcance de su utilización y su justificación. Esos exámenes siempre deben incluir un análisis de la compatibilidad de la práctica de los Estados con los requisitos del Pacto.

49. Además de este tipo de revisión general, los Estados tienen la obligación específica de poner recursos a disposición de las personas que consideren que sus derechos reconocidos en el Pacto han sido vulnerados. El artículo 2, párrafo 3 b), del Pacto establece que los Estados partes deben garantizar que toda persona que interponga un recurso goce del derecho jurídicamente exigible de que una autoridad competente interna, de carácter judicial, administrativo o legislativo, decida sobre su recurso. Para hacer este derecho efectivo, la legislación nacional debe prever un mecanismo independiente capaz de efectuar un examen exhaustivo e imparcial, con acceso a todo el material pertinente y con las garantías procesales adecuadas, que tenga la potestad de atender los recursos interpuestos con efectos vinculantes (como, por ejemplo, cuando proceda, ordenando el cese de la vigilancia o la destrucción del producto) (véase A/HRC/14/46; y A/HRC/27/37, párr. 39).

50. Para invocar el derecho a un recurso efectivo generalmente es necesario que la persona demuestre que sus derechos han sido vulnerados. En el contexto de las medidas de vigilancia secreta, este requisito puede ser difícil o imposible de alcanzar. Muy pocos Estados cuentan con disposiciones que exijan que se notifique al sospechoso que se lo ha vigilado. Por ello, el Tribunal Europeo de Derechos Humanos flexibilizó el requisito por el cual la persona debía demostrar que había sido sometida a vigilancia secreta. El Tribunal distingue entre las demandas por la existencia de un régimen que presuntamente no se ajusta a lo dispuesto en el Convenio Europeo de Derechos Humanos, y las demandas por casos concretos de actividad ilegal del Estado. En el primer caso, el Tribunal ha estado dispuesto a examinar las disposiciones impugnadas en sí mismas[35], mientras que, en el segundo, en general ha exigido que los demandantes demuestren una "probabilidad razonable" de que han sido vigilados de manera ilegal[36]. En el contexto de los regímenes de vigilancia a gran escala, el Relator Especial considera que cualquier usuario de Internet debería estar legitimado para impugnar la legalidad, la necesidad y la proporcionalidad de las medidas en cuestión.

7. La necesidad y la proporcionalidad de los programas de vigilancia a gran escala

51. Corresponde a los Estados demostrar que una injerencia en el derecho a la privacidad reconocido en el artículo 17 del Pacto es un medio necesario para alcanzar un objetivo legítimo. Para ello, es preciso que exista un vínculo racional entre los medios utilizados y el objetivo perseguido, y que la medida escogida sea "el instrumento menos perturbador de los que permitan conseguir el resultado deseado" (véase CCPR/C/21/Rev.1/Add.9; y A/HRC/13/37, párr. 60). El principio de proporcionalidad conexo implica equilibrar el alcance de la intrusión en los derechos a la privacidad en Internet con el beneficio específico para las investigaciones llevadas adelante por una autoridad pública en interés público. No

[35] *Klass v. Germany*, EHRR 1979-80, vol. 2, pág. 214.

[36] *Halford v. United Kingdom*, EHRR 1997, vol. 24, pág. 523.

obstante, el grado permitido de injerencia en un derecho amparado en el Pacto tiene ciertos límites. Como subrayó el Comité de Derechos Humanos, "en ningún caso se deben aplicar las restricciones o invocarse de una manera que menoscabe la esencia de un derecho del Pacto"[37]. En el contexto de la vigilancia encubierta, el Comité, por tanto, ha destacado que las decisiones que autoricen la intervención de las comunicaciones deben ser adoptadas por la autoridad designada por la ley tras examinar "cada caso en particular"[38]. La proporcionalidad de toda injerencia en el derecho a la privacidad, por lo tanto, debe juzgarse según las circunstancias particulares del caso concreto[39].

52. El uso de tecnología de vigilancia a gran escala por parte de los Estados no encaja con ninguno de estos principios. La capacidad técnica para ejecutar programas de recopilación y análisis de grandes cantidades de datos es sin duda un medio adicional para realizar investigaciones en el marco de la lucha contra el terrorismo y de la aplicación de la ley. Sin embargo, una evaluación de la proporcionalidad de estos programas también debe tener en cuenta el daño colateral a los derechos a la privacidad colectivos. Los programas de recopilación de datos a gran escala al parecer contradicen el requisito según el cual los organismos de inteligencia deben elegir la medida menos perturbadora para los derechos humanos (a menos que los Estados pertinentes estén en condiciones de demostrar que únicamente el acceso irrestricto a todas las comunicaciones por Internet sería suficiente para proporcionar protección contra la amenaza del terrorismo y otros delitos graves). Dado que no hay oportunidad de evaluar individualmente la proporcionalidad antes de recurrir a estas medidas, estos programas al parecer también vulneran la propia esencia del derecho a la privacidad. Excluyen por completo el análisis de "cada caso en particular" que el Comité de Derechos Humanos consideró esencial y, por tal motivo, pueden considerarse arbitrarios, aunque persigan un objetivo legítimo y hayan sido aprobados sobre la base de un régimen jurídico accesible (véase A/HRC/27/37, párr. 25). El Relator Especial llega entonces a la conclusión de que esos programas pueden ser compatibles con el artículo 17 del Pacto únicamente si los Estados pertinentes estuvieran en condiciones de justificar la injerencia sistemática en el derecho a la privacidad en Internet de un número potencialmente ilimitado de personas inocentes en cualquier parte del mundo por considerarla proporcional[40].

8. La legislación de conservación obligatoria de datos y la extracción automatizada de los datos de tráfico de las comunicaciones en poder de los proveedores de servicios de telecomunicaciones e Internet

53. Los programas de vigilancia a gran escala no se circunscriben a la intervención del contenido de las comunicaciones. Las comunicaciones digitales generan grandes cantidades de datos de transacciones. Estos datos de tráfico de las comunicaciones

[37] Observaciones generales núms. 27 y 31 del Comité de Derechos Humanos.

[38] Observación general núm. 16 del Comité de Derechos Humanos, párr. 8.

[39] Observación general núm. 16 del Comité de Derechos Humanos, párr. 4, *Van Hulst c. los Países Bajos*, Comunicación núm. 903/1999, 2004, párr. 7.3; *Toonen c. Australia*, Comunicación núm. 488/1992, párr. 8.3.

[40] Véase A/HRC/27/37, párr. 25, en el que la Alta Comisionada para los Derechos Humanos observó que "no es suficiente que las medidas tengan por objeto encontrar determinadas agujas en un pajar; lo importante es el impacto de las medidas en el pajar, en comparación con el riesgo de que se trate; es decir, si la medida es necesaria y proporcionada".

(o metadatos) comprenden información personal de los particulares, su ubicación y sus actividades en línea. Muchos Estados han promulgado leyes que obligan a los proveedores de servicios de telecomunicaciones e Internet a recopilar y conservar los datos de tráfico de las comunicaciones para que posteriormente estén disponibles para su análisis. Esas leyes suelen exigir a los proveedores de servicios que proporcionen a las autoridades estatales información sobre la distribución de las direcciones de protocolo de Internet, que permiten identificar al usuario de una dirección en particular en cualquier momento. La captura de los datos de tráfico de las comunicaciones es una herramienta cada vez más valiosa para los Estados. Estos datos se almacenan y registran con facilidad, y pueden utilizarse para crear perfiles de las personas que son tan privados como el contenido de las comunicaciones (véase A/HRC/27/37, párr. 19). Al combinar y agrupar la información derivada de los datos de tráfico de las comunicaciones, es posible determinar la ubicación de una persona, sus asociaciones y sus actividades (véase A/HRC/23/40, párr. 15). En ausencia de salvaguardas especiales, prácticamente no existe una dimensión secreta de la vida privada de una persona que pueda resistir un análisis pormenorizado de los metadatos[1]. Por ello, la extracción automatizada de datos tiene un efecto particularmente corrosivo en la privacidad.

54. En muchos Estados, una gran cantidad de organismos públicos tienen acceso a los datos de tráfico de las comunicaciones, para una amplia variedad de fines, a menudo sin autorización judicial o sin supervisión independiente y sustancial. En el Reino Unido, por ejemplo, más de 200 organismos están autorizados para solicitar datos de tráfico de las comunicaciones con arreglo a la Ley de Reglamentación de las Facultades de Investigación de 2000[41], y solamente en 2013 las autoridades públicas presentaron 514.608 solicitudes de datos de tráfico de las comunicaciones[42]. Los tribunales reconocen desde hace algún tiempo que la entrega de metadatos a una autoridad pública constituye una injerencia en el derecho a la privacidad, y el Tribunal de Justicia de la Unión Europea afirmó recientemente que la conservación de los metadatos relativos a la vida privada de una persona y a sus comunicaciones constituía en sí misma una injerencia en el derecho[43] (y que permitir el acceso a los metadatos conservados para su análisis constituía una clara injerencia adicional)[44]. Al arribar a esta conclusión, el Tribunal de Justicia de la Unión Europea destacó que con los metadatos de las comunicaciones se podían "extraer conclusiones muy precisas sobre la vida privada de las personas cuyos datos se han conservado"[45].

55. Al aplicar el enfoque adoptado por el Tribunal de Justicia de la Unión Europea se desprende que la recopilación y conservación de los datos de tráfico de las comunicaciones constituye una injerencia en el derecho a la privacidad, independientemente de si posteriormente una autoridad pública accede a ellos y los analiza o no. Ni la captura de los datos de tráfico de las comunicaciones prevista en la legislación que obliga a su conservación, ni su posterior entrega a las autoridades

[41] La lista de organismos autorizados a solicitar datos de tráfico de las comunicaciones comprende a las autoridades fiscales y los organismos gubernamentales locales, y puede ampliarse por legislación delegada (decreto del poder ejecutivo).

[42] Véase www.intelligencecommissioners.com/.

[43] Tribunal de Justicia de la Unión Europea, sentencia de 8 de abril de 2014 en los asuntos acumulados C-293/12 y C-594/12, *Digital Rights Ireland Ltd y Seitlinger y otros*, párr. 34.

[44] *Ibid*., párr. 35.

[45] *Ibid*., párrs. 26, 27 y 37.

estatales (y el análisis realizado por estas), requiere que se sospeche previamente de una persona u organización en particular. Por lo tanto, el Relator Especial comparte las reservas expresadas por la Alta Comisionada con respecto a la necesidad y proporcionalidad de las leyes de conservación obligatoria de los datos (véase A/HRC/27/37, párr. 26).

9. Especificación de la finalidad

56. Muchos Estados carecen de disposiciones relativas a la "especificación de la finalidad" que impidan que la información obtenida con una finalidad se utilice para otros objetivos gubernamentales inconexos. Como consecuencia de ello, los datos recopilados aparentemente con fines relacionados con la seguridad nacional pueden ser compartidos por los organismos de inteligencia, los organismos encargados de hacer cumplir la ley y otras entidades del Estado, incluidas las autoridades fiscales, los consejos locales y los órganos que otorgan licencias[46]. Los organismos de seguridad nacional y encargados de hacer cumplir la ley a menudo son exceptuados de las disposiciones de la legislación de protección de datos que limitan el intercambio de datos personales. Debido a ello, a los particulares les puede resultar difícil prever qué organismo estatal podría vigilarlos y cuándo. Esta "expansión de la finalidad" podría vulnerar el artículo 17 del Pacto, no solo porque la legislación pertinente carece de previsibilidad, sino también porque las medidas de vigilancia que podrían ser necesarias y proporcionales para un objetivo legítimo podrían no serlo para otro (*ibid.*, párr. 27). Por lo tanto, el Relator Especial hace suya la recomendación de su predecesor de exigir a los Estados que proporcionen un fundamento jurídico para reutilizar la información personal, de conformidad con los principios de los derechos humanos (véase A/HRC/13/37, párrs. 50 y 66). Esto es de particular importancia cuando la información se comparte a través de las fronteras o con otros Estados.

10. El sector privado

57. Los Estados recurren cada vez más al sector privado para facilitar la vigilancia digital. Esta práctica no se limita a la promulgación de leyes de conservación obligatoria de los datos. Las empresas también han sido cómplices directas del uso de la tecnología de acceso masivo al diseñar la infraestructura de comunicaciones que facilita la vigilancia a gran escala. Los proveedores de servicios de telecomunicaciones e Internet se han visto obligados a hacer que sus tecnologías sean vulnerables para que puedan ser intervenidas. La Alta Comisionada para los Derechos Humanos ha considerado que estas prácticas constituyen una "delegación de las responsabilidades policiales y cuasijudiciales a los intermediarios de Internet disfrazada de autorregulación o cooperación" (véase A/HRC/27/37, párr. 42). El Relator Especial está de acuerdo con esta apreciación. Para no ser cómplices de violaciones de los derechos humanos, los proveedores de servicios deben velar por que sus operaciones se ajusten a los Principios Rectores sobre las Empresas y los Derechos Humanos, aprobados por el Consejo de Derechos Humanos en 2011 (*ibid.*, párrs. 43 a 46).

---

[46] Se puede consultar el análisis sobre las formas en que se ha dado el fenómeno de la expansión de la finalidad en el Reino Unido en www.whatdotheyknow.com/request/127491/response/315758/attach/html/2/Summay%20of%20Counsels%20advice.pdf.html.

IV. Conclusiones y recomendaciones

58. **Las obligaciones que incumben a los Estados en virtud del artículo 17 del Pacto Internacional de Derechos Civiles y Políticos comprenden la obligación de respetar la privacidad y la seguridad de las comunicaciones digitales. Esto supone, en principio, que las personas tienen derecho a compartir información e ideas entre sí sin la injerencia del Estado, con la certeza de que sus comunicaciones llegarán a sus destinatarios y solo estos las leerán. Las medidas que constituyen una injerencia en este derecho deben ser autorizadas por una ley nacional que sea accesible y precisa y que se ajuste a los requisitos del Pacto. Deben además tener un objetivo legítimo y cumplir los criterios de necesidad y proporcionalidad**.

59. **La prevención y represión del terrorismo es un imperativo de interés público que reviste la mayor importancia y podría ser, en principio, una justificación plausible de la vigilancia de Internet a gran escala. Sin embargo, el alcance técnico de los programas vigentes es tan amplio que estos podrían ser compatibles con el artículo 17 del Pacto únicamente si los Estados pertinentes estuvieran en condiciones de justificar la injerencia sistemática en el derecho a la privacidad en Internet de un número potencialmente ilimitado de personas inocentes en cualquier parte del mundo por considerarla proporcional. La tecnología de acceso masivo menoscaba indiscriminadamente la privacidad en línea e infringe la esencia misma del derecho garantizado en el artículo 17. En ausencia de una derogación formal de las obligaciones de los Estados impuestas por el Pacto, estos programas representan una amenaza directa y permanente para una norma establecida de derecho internacional**.

60. **El Relator Especial está de acuerdo con la Alta Comisionada para los Derechos Humanos en que urge que los Estados que utilizan esta tecnología revisen y actualicen la legislación nacional para que se ajuste al derecho internacional de los derechos humanos. No solo se trata de un requisito previsto en el artículo 17, sino que también ofrece una importante oportunidad de celebrar un debate fundado que cree conciencia pública y permita que las personas tomen decisiones con conocimiento de causa. Cuando los derechos a la privacidad de toda la comunidad digital están en peligro, se requiere como mínimo una normativa exhaustiva y expresa promulgada por el poder legislativo. Se deberían imponer restricciones adecuadas al uso que puede darse a los datos recopilados, exigiendo a las autoridades competentes que ofrezcan un fundamento jurídico para la reutilización de la información personal**.

61. **Los Estados deberían establecer órganos de supervisión independientes y sólidos que cuenten con recursos suficientes y con el mandato de llevar a cabo exámenes previos, analizando las solicitudes de autorización no solo teniendo en cuenta los requisitos de la legislación nacional, sino también los requisitos de necesidad y proporcionalidad del Pacto. Además, las personas deberían tener derecho a interponer recursos efectivos cuando sus derechos a la privacidad en línea sean presuntamente vulnerados. Para ello es necesario contar con un medio por el cual las personas afectadas puedan interponer recursos ante un mecanismo independiente que sea capaz de efectuar un examen exhaustivo e imparcial, con acceso a todo el material pertinente y con las garantías procesales adecuadas. Si bien los mecanismos de rendición de cuentas pueden revestir diversas formas, deben ser capaces de contemplar recursos con efectos**

vinculantes. Los Estados no deberían imponer requisitos permanentes que menoscaben el derecho a un recurso efectivo.

62. **El Relator Especial está de acuerdo con la Alta Comisionada para los Derechos Humanos en que cuando los Estados penetran la infraestructura que se encuentra fuera de su jurisdicción territorial, siguen estando sujetos a las obligaciones que les incumben en virtud del Pacto. Además, el artículo 26 del Pacto prohíbe la discriminación por motivos de nacionalidad y ciudadanía, entre otros. Por lo tanto, el Relator Especial considera que los Estados están obligados jurídicamente a proporcionar igual protección de la privacidad a ciudadanos y extranjeros, y a quienes se encuentren dentro y fuera de su jurisdicción. Los regímenes de protección asimétrica de la privacidad constituyen una violación flagrante de los requisitos del Pacto**.

63. **El Relator Especial exhorta a todos los Estados que utilizan actualmente tecnología de vigilancia digital a gran escala a que proporcionen una justificación exhaustiva, pública y fundada en pruebas de la injerencia sistemática en los derechos a la privacidad de la comunidad en línea en función de los requisitos contemplados en el artículo 17 del Pacto. Los Estados deberían ser claros con respecto a la naturaleza y el alcance de su penetración en Internet, su metodología y su justificación, y deberían comunicar públicamente y en detalle los beneficios tangibles que se derivan de su uso**.

64. **El Relator Especial está de acuerdo con su predecesor (véase A/HRC/13/37, párr. 19) y con el anterior Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión (véase A/HRC/23/40, párr. 98) en que el Comité de Derechos Humanos debería preparar y aprobar una nueva observación general sobre el derecho a la privacidad en línea que refleje la evolución de la vigilancia de las comunicaciones digitales desde que se aprobó la observación general núm. 16 en 1988**.