Naciones Unidas A/HRC/23/40

Asamblea General

Distr. general
17 de abril de 2013
Español
Original: inglés

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

Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, Frank La Rue*

Resumen

En el presente informe, que se remite de conformidad con la resolución 16/4 del Consejo de Derechos Humanos, se analizan las consecuencias de la vigilancia de las comunicaciones por los Estados en el ejercicio de los derechos humanos a la intimidad y a la libertad de opinión y expresión. Al tiempo que se analizan los efectos de los importantes adelantos tecnológicos en las comunicaciones, en el informe se subraya la necesidad urgente de seguir estudiando nuevas modalidades de vigilancia y de examinar las leyes nacionales que reglamentan estas prácticas de conformidad con las normas de derechos humanos.

* Documento presentado con retraso.

GE.13-13306 (S) 121114 131114
1313306

Índice

I. Introducción

1. En el presente informe se analizan las consecuencias de la vigilancia de las comunicaciones por los Estados en el ejercicio de los derechos humanos a la intimidad y a la libertad de opinión y expresión. Al tiempo que se analizan los efectos de los importantes adelantos tecnológicos en las comunicaciones, en el informe se subraya la necesidad urgente de seguir estudiando nuevas modalidades de vigilancia y de examinar las leyes nacionales que reglamentan estas prácticas de conformidad con las normas de derechos humanos.

2. Las innovaciones tecnológicas han aumentado las posibilidades de comunicación y la protección de la libre expresión y opinión, permitiendo el anonimato, el rápido intercambio de información y el diálogo intercultural. Al mismo tiempo, los cambios tecnológicos han incrementado las oportunidades de vigilancia por los Estados y las intervenciones en las comunicaciones privadas de las personas.

3. Las preocupaciones relativas a la seguridad nacional y la actividad delictiva podrían justificar el uso excepcional de tecnologías de vigilancia de las comunicaciones. No obstante, las leyes nacionales que reglamentan qué constituiría la participación necesaria, legítima y proporcional del Estado en la vigilancia de las comunicaciones suelen ser insuficientes o inexistentes. Los marcos jurídicos nacionales inadecuados propician la vulneración ilícita del derecho a la intimidad en las comunicaciones y, por consiguiente, también amenazan la protección del derecho a la libertad de opinión y expresión.

4. En informes anteriores (A/HRC/17/27 y A/66/290), el Relator Especial analizó las repercusiones sin precedentes de Internet en el aumento de las posibilidades de las personas a ejercer su derecho a la libertad de opinión y expresión. Manifestó su preocupación respecto de las múltiples medidas adoptadas por los Estados para impedir o restringir el flujo de información en línea, y destacó la protección insuficiente del derecho a la intimidad en Internet.

5. El presente informe, que se basa en el análisis previo, tiene por objeto determinar los riesgos que los nuevos medios y modalidades de vigilancia de las comunicaciones plantean para los derechos humanos, incluido el derecho a la intimidad y a libertad de opinión y expresión.

6. En el presente informe se utilizan los términos que se enumeran a continuación para describir las modalidades más comunes de vigilancia de las comunicaciones:

a) Vigilancia de las comunicaciones: el seguimiento, la interceptación, la recopilación, conservación y retención de información que ha sido comunicada, transmitida o generada a través de redes de comunicación;

b) Datos de las comunicaciones: la información acerca de las comunicaciones personales (correos electrónicos, llamadas telefónicas y mensajes de texto enviados y recibidos, mensajes y publicaciones en redes sociales), identidad, cuentas de usuarios de red, direcciones, sitios web visitados, libros y otro material consultado, mirado o escuchado, búsquedas realizadas, recursos utilizados, interacciones (origen y destino de las comunicaciones, personas con las que se interactuó, amigos, familiares, conocidos), y horario y ubicación del usuario, incluida la proximidad con otras personas);

c) Filtrado de la información contenida en Internet: seguimiento automático o manual del contenido en Internet (incluidos sitios web, *blogs* y medios de información en línea, así como correo electrónico) para restringir o suprimir determinados textos, imágenes, sitios web, redes, protocolos, servicios o actividades.

II. Actividades del Relator Especial

7. En el período de que se informa, el Relator Especial participó en múltiples actividades internacionales y nacionales relacionadas con cuestiones tratadas en sus informes anteriores como la libertad de expresión en Internet, la prevención de la expresión del odio y la protección de periodistas. Prestó atención especial a las iniciativas nacionales para promover la protección de periodistas; en tal sentido, participó en reuniones sobre iniciativas adoptadas en el Brasil, Colombia, Honduras y México. Además, asistió a la Reunión Interinstitucional de las Naciones Unidas sobre la Seguridad de los Periodistas y la Cuestión de la Impunidad, que se celebró en noviembre de 2012 en Viena.

8. Su último informe a la Asamblea General de las Naciones Unidas se centró en la prevención de la expresión del odio y la incitación al odio[1]. El mismo tema se abordó en una actividad paralela de la Asamblea General organizada conjuntamente por el Relator Especial y el Asesor Especial sobre la Prevención del Genocidio en febrero de 2013. El mismo mes, también trató estas cuestiones en la presentación del Plan de Acción de Rabat sobre la prohibición de la apología del odio nacional, racial o religioso que constituye incitación a la discriminación, la hostilidad o la violencia, realizada en Ginebra y en el quinto Foro Mundial de la Alianza de Civilizaciones de las Naciones Unidas celebrado en Viena.

9. El Relator Especial llevó a cabo una misión a Honduras del 7 al 14 de agosto de 2012. Sus principales conclusiones y recomendaciones sobre esta visita figuran en la adición al presente informe (A/HRC/20/40/Add.1). El Gobierno de Indonesia lo invitó a visitar el país en enero de 2013. Lamentablemente, el Gobierno solicitó el aplazamiento de la visita y aún no se han confirmado las nuevas fechas de esta.

10. Para la preparación del presente informe, el Relator Especial examinó los estudios pertinentes y celebró consultas con expertos sobre cuestiones relacionadas con la vigilancia de las comunicaciones. En diciembre de 2012 participó en el Taller sobre Vigilancia Electrónica y Derechos Humanos organizado por la Electronic Frontier Foundation. En febrero de 2013 el Relator Especial realizó una consulta de expertos para la preparación del presente informe, que se celebró paralelamente a las actividades de la Cumbre Mundial sobre la Sociedad de la Información (CMSI+10) en la sede de la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) en París, en la que el Relator Especial también participó en el grupo plenario de apertura.

III. Evolución de la tecnología de vigilancia

11. Las innovaciones tecnológicas han creado mayores oportunidades de comunicación y libertad de expresión, facilitando el anonimato, el rápido intercambio de información y el diálogo intercultural. Al mismo tiempo, los cambios tecnológicos también ofrecen nuevas oportunidades de vigilancia e intervención del Estado en las vidas privadas de las personas.

12. Desde la aparición de la primera forma de comunicaciones remotas, los Estados han procurado interceptar y vigilar las comunicaciones personales para responder a los intereses de las fuerzas del orden y de la seguridad nacional. Las comunicaciones permiten revelar la información más personal e íntima, inclusive acerca de las actividades pasadas o futuras de una persona o un grupo. Las comunicaciones representan una valiosa fuente de datos que el Estado puede utilizar para prevenir o enjuiciar delitos graves o evitar posibles emergencias de seguridad nacional.

[1] A/67/357.

13. La innovación tecnológica a lo largo de todo el siglo XX cambió la naturaleza y las repercusiones de la vigilancia de las comunicaciones. Los medios por los cuales las personas se comunican y la frecuencia con que pueden hacerlo se han ampliado considerablemente. La transición de los sistemas de telefonía fija a las telecomunicaciones móviles y la rebaja de los costos de los servicios de comunicación dieron lugar a un crecimiento notable del uso de la telefonía. Con la aparición de Internet surgieron nuevas herramientas y aplicaciones de comunicación sin costo alguno, o a precios sumamente asequibles. Estos adelantos han posibilitado una mayor conectividad, facilitado el flujo mundial de información e ideas, y el aumento de las oportunidades de crecimiento económico y cambio social.

14. Las tecnologías de la información y las comunicaciones evolucionaron en forma paralela a los medios por los cuales los Estados procuraron hacer el seguimiento de las comunicaciones privadas. Al aumentar el uso de los teléfonos, comenzaron las escuchas telefónicas, que consisten en la colocación de un dispositivo de interceptación en los cables telefónicos para escuchar conversaciones telefónicas privadas. Mediante la sustitución de redes telefónicas analógicas por fibra óptica y centralitas telefónicas digitales en la década de 1990, los Estados rediseñaron la tecnología de redes para incluir la capacidad de interceptación ("puertas traseras") que permite la vigilancia, posibilitando el acceso y el control remotos a las redes telefónicas modernas.

15. El carácter dinámico de la tecnología no solo ha cambiado la forma en que puede llevarse a cabo la vigilancia, sino también "qué" puede vigilarse. Al facilitar la creación de oportunidades de comunicación e intercambio de información, Internet también ha posibilitado la elaboración de un gran volumen de datos de transacciones de personas y acerca de estas. Esta información, conocida como datos de las comunicaciones o metadatos, incluye información personal sobre particulares, su ubicación y actividades en línea, así como registros e información conexa sobre los correos electrónicos y los mensajes que envían o reciben. Los datos de las comunicaciones pueden almacenarse, son accesibles y permiten la realización de búsquedas, y su revelación a las autoridades públicas y su utilización por estas están en gran medida no reguladas. El análisis de estos datos puede ser sumamente revelador e invasivo, en particular cuando los datos se combinan y acumulan. En tal sentido, los Estados se basan cada vez más en datos de las comunicaciones para prestar apoyo a las investigaciones de las fuerzas del orden o de seguridad nacional. Los Estados también están disponiendo la obligatoriedad de conservar y retener los datos de las comunicaciones para poder llevar a cabo una vigilancia histórica.

16. Los cambios tecnológicos han estado acompañados de cambios de actitud hacia la vigilancia de las comunicaciones. Cuando comenzó a utilizarse por primera vez la práctica de las escuchas telefónicas oficiales en los Estados Unidos de América, se usó en forma restringida y los tribunales eran renuentes a autorizarlas[2]. Se consideraban una amenaza tan seria al derecho a la intimidad que su uso debía limitarse a la detección y el enjuiciamiento de los delitos más graves. Sin embargo, con el tiempo los Estados han ampliado sus atribuciones para llevar a cabo vigilancias, reduciendo las restricciones y aumentando las justificaciones de dicha vigilancia.

[2] En la primera validación judicial de las escuchas telefónicas, el Juez Brandeis del Tribunal Supremo de los Estados Unidos expresó su disensión en forma mordaz al afirmar que las escuchas telefónicas eran "un medio más sutil y de mucho mayor alcance de invadir la privacidad" que no podían justificarse en el marco de la Constitución. En un pronóstico de precisión aterradora, el eminente jurista predijo: "Algún día el Gobierno podría encontrar formas para reproducir documentos ante un tribunal, sin necesidad de extraerlos de cajones secretos, y de este modo, exponer ante un jurado los acontecimientos más íntimos de un hogar. Los avances en materia de psicología y otras ciencias conexas podrían aportar medios para explorar creencias, pensamientos y emociones no expresados". *Olmstead v. United States*, 277 U.S. 438 (1928).

17. En muchos países, no se han examinado ni actualizado las leyes y prácticas vigentes para hacer frente a las amenazas y retos de la vigilancia de las comunicaciones en la era digital. Así pues, las nociones tradicionales de acceso a la correspondencia escrita se han trasladado a leyes que permiten el acceso a las computadoras personales y otras tecnologías de la información y las comunicaciones, sin tener en cuenta los usos ampliados de estos dispositivos y las consecuencias que tienen en los derechos de las personas. Al mismo tiempo, la ausencia de leyes que regulen la vigilancia mundial de las comunicaciones y los acuerdos de intercambio de información han dado lugar a prácticas especiales que están fuera del alcance de la supervisión de una autoridad independiente. Actualmente en muchos Estados, un gran número de órganos públicos pueden obtener acceso a datos de las comunicaciones con distintas finalidades, a menudo sin autorización judicial ni supervisión independiente. Además, los Estados han procurado adoptar disposiciones de vigilancia que pretenden tener efecto extraterritorial.

18. Los mecanismos de derechos humanos también han sido lentos para evaluar las repercusiones de Internet y las nuevas tecnologías de vigilancia de las comunicaciones y el acceso a datos de las comunicaciones en los derechos humanos. Las consecuencias de ampliar las atribuciones y prácticas de vigilancia de los Estados en los derechos a la intimidad y la libertad de opinión y expresión, y la dependencia mutua entre estos dos derechos aún deberán ser objeto de un examen detenido por el Consejo de Derechos Humanos, los titulares de mandatos de procedimientos especiales o los órganos creados en virtud de tratados de derechos humanos. El presente informe tiene por objeto subsanar esta deficiencia.

IV. Marco internacional de derechos humanos

19. El derecho a la libertad de opinión y expresión se garantiza en virtud de los artículos 19 de la Declaración Universal de Derechos Humanos y del Pacto Internacional de Derechos Civiles y Políticos, que afirman que todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión. A nivel regional, el derecho está protegido por la Carta Africana de Derechos Humanos y de los Pueblos (art. 9), la Convención Americana sobre Derechos Humanos (art. 13); y el Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales (art. 10).

20. El derecho a la vida privada también se reconoce inequívocamente tanto a nivel internacional como regional como un derecho humano fundamental. Se consagra en la Declaración Universal de Derechos Humanos (art. 12), el Pacto Internacional de Derechos Civiles y Políticos (art. 17), la Convención sobre los Derechos del Niño (art. 16), y la Convención Internacional sobre la Protección de los Derechos de Todos los Trabajadores Migratorios y de sus Familiares (art. 14). A nivel regional, el derecho a la vida privada está protegido por el Convenio Europeo de Derechos Humanos (art. 8) y la Convención Americana sobre Derechos Humanos (art. 11).

21. Pese al reconocimiento generalizado de la obligación de proteger la vida privada, los mecanismos internacionales de protección de los derechos humanos no elaboraron plenamente el contenido concreto de este derecho en el momento de su inclusión en los instrumentos de derechos humanos que se mencionan más arriba. La ausencia de una formulación explícita del contenido de este derecho ha traído aparejadas dificultades en su aplicación y cumplimiento[3]. Habida cuenta de que el derecho a la vida privada es un derecho condicionado, su interpretación plantea desafíos respecto de qué constituye la

[3] UNESCO, *Global Survey on Internet Privacy and Freedom of Expression*, 2012, pág. 51.

esfera privada y el establecimiento de nociones sobre qué constituye el interés público. Los cambios rápidos y trascendentales en las tecnologías de la información y las comunicaciones registrados en los últimos decenios también han afectado de manera irreversible a nuestra comprensión de los límites entre las esferas pública y privada.

22. La intimidad se define como la presunción de que el individuo debe tener una esfera de desarrollo autónomo, interacción y libertad, una "esfera privada" con o sin relación con otros y libre de la intervención del Estado y de la intervención excesiva no solicitada de otros individuos no invitados[4]. El derecho a la intimidad también es la capacidad de las personas para determinar quién posee información acerca de ellos y cómo se utiliza dicha información.

23. Si es que las personas han de ejercer su derecho a la intimidad en el ámbito de las comunicaciones, deben estar en condiciones de garantizar que estas sean privadas, seguras y, si así lo desean, anónimas. La confidencialidad de las comunicaciones supone que las personas pueden intercambiar información en un ámbito que está fuera del alcance de otros miembros de la sociedad, el sector privado y, en última instancia, el propio Estado. La seguridad de las comunicaciones implica que las personas deberían poder verificar que sus comunicaciones sean recibidas únicamente por los destinatarios a las que están dirigidas, sin injerencias ni modificaciones, y que todas las comunicaciones que reciban estén también libres de injerencias. El anonimato de las comunicaciones es uno de los adelantos más importantes facilitados por Internet, que permite a las personas expresarse libremente sin temor a represalias o condenas.

A. Relación recíproca entre el derecho a la intimidad y el derecho a la libertad de opinión y expresión

24. El derecho a la intimidad suele entenderse como un requisito esencial para la realización del derecho a la libertad de expresión. La injerencia indebida en la intimidad de las personas puede limitar en forma tanto directa como indirecta el libre intercambio y evolución de ideas. Las restricciones al anonimato de las comunicaciones, por ejemplo, tienen un efecto intimidatorio en las víctimas de todas las formas de violencia y abuso, que podrían ser renuentes a denunciarlas por temor a la doble victimización. En tal sentido, el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos se refiere directamente a la protección de injerencias en su "correspondencia", un término cuya interpretación debería abarcar todas las formas de comunicación, dentro y fuera de Internet[5]. Como lo observó el Relator Especial en un informe anterior[6], el derecho a la correspondencia privada genera una amplia obligación del Estado de velar por que el correo electrónico y otras formas de comunicación en línea lleguen a su destinatario previsto sin injerencia o inspección por parte de órganos estatales o de terceros[7].

25. El Comité de Derechos Humanos analizó el contenido del derecho a la intimidad (art. 17) en su observación general Nº 16 (1988), según la cual en el artículo 17 del Pacto se prevé el derecho de toda persona a ser protegida respecto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, y los marcos jurídicos nacionales deben prever la protección de este derecho. Esta disposición impone obligaciones concretas relativas a la protección de la confidencialidad de las comunicaciones y subraya que "[l]a correspondencia debe ser entregada al destinatario sin

[4] Lord Lester y D. Pannick (eds.). *Human Rights Law and Practice.* Londres, Butterworth, 2004, párr. 4.82.

[5] ICCPR commentary, pág. 401.

[6] A/HRC/17/23.

[7] ICCPR commentary, pág. 401.

ser interceptada ni abierta o leída de otro modo. Debe prohibirse la vigilancia, por medios electrónicos o de otra índole, la intervención de las comunicaciones telefónicas, telegráficas o de otro tipo, así como la intervención y grabación de conversaciones"[8]. La observación general también indica que "la recopilación y el registro de información personal en computadoras, bancos de datos y otros dispositivos, tanto por las autoridades públicas como por las particulares o entidades privadas, deben estar reglamentados por la ley"[9]. En el momento en que se aprobó esta observación general, apenas se comprendía la repercusión de los adelantos en materia de tecnologías de la información y las comunicaciones sobre el derecho a la intimidad.

26. En su observación general Nº 34 (2011) sobre libertad de opinión y libertad de expresión, el Comité de Derechos Humanos indicó que los Estados partes deberían tener en cuenta la medida en que la evolución de las tecnologías de la información y la comunicación han cambiado sustancialmente las prácticas de la comunicación. El Comité también instó a los Estados partes a tomar todas las medidas necesarias para fomentar la independencia de esos nuevos medios. La observación general también analiza la relación entre la protección de la vida privada y la libertad de expresión y recomienda que los Estados partes respeten el elemento del derecho a la libertad de expresión que comprende la prerrogativa limitada de los periodistas de no revelar sus fuentes de información[10].

27. También se plantean conflictos entre el derecho a la intimidad y el derecho a la libertad de expresión, por ejemplo, cuando información considerada de la vida privada se difunde a través de los medios de comunicación. En este sentido, el artículo 19 3) del Pacto Internacional de Derechos Civiles y Políticos establece restricciones a la libertad de expresión e información para proteger los derechos de los demás. Sin embargo, lo cierto es que en todas las limitaciones permisibles del derecho a la libertad de expresión (véase más abajo), debe observarse estrictamente el principio de proporcionalidad pues de lo contrario se corre peligro de que se socave la libertad de expresión. En particular, en el ámbito político no deben permitirse todos los ataques a la buena reputación de los políticos, ya que de lo contrario la libertad de expresión e información quedaría despojada de su importancia fundamental para el proceso de formación de opiniones políticas[11], el fomento de la transparencia y la lucha contra la corrupción. La jurisprudencia internacional a nivel regional indica que en situaciones de conflicto entre la intimidad y la libertad de expresión, debería hacerse referencia al interés público general en relación con los asuntos de que se informa[12].

B. Limitaciones permisibles a la vida privada y la libertad de expresión

28. El marco del artículo 17 del Pacto Internacional de Derechos Civiles y Políticos prevé restricciones necesarias, legítimas y proporcionales al derecho a la vida privada mediante limitaciones permisibles. A diferencia de las disposiciones del artículo 19, párrafo 3, que contienen los elementos necesarios para unas limitaciones permisibles[13], la

[8] Centro de Derechos Civiles y Políticos, observación general Nº 16 (observaciones generales), párr. 8.

[9] *Ibid.*, párr. 10.

[10] Observación general Nº 34 del Comité de Derechos Humanos.

[11] Nowak, Manfred, Pacto Internacional de Derechos Civiles y Políticos: CCPR Commentary (1993), pág. 462.

[12] UNESCO, *Global Survey on Internet Privacy and Freedom of Expression*, 2012, págs. 53 y 99.

[13] También se enumeran limitaciones permisibles en el artículo 12 3), sobre el derecho a circular libremente por el territorio de un Estado y a escoger libremente en él su residencia; el artículo 18 3), sobre el derecho a la libertad de pensamiento, de conciencia y de religión; el artículo 21, sobre el derecho de reunión pacífica; y el artículo 22 2), sobre el derecho a asociarse libremente.

formulación del artículo 17 no contiene una cláusula de limitación. Pese a estas diferencias de redacción, se entiende que el artículo 17 del Pacto también se debe interpretar en el sentido de que contiene los elementos necesarios para unas limitaciones admisibles que ya se describen en otras observaciones generales del Comité de Derechos Humanos[14].

29. En este sentido, el Relator Especial sostiene que el derecho a la vida privada debería estar sujeto a las mismas limitaciones admisibles que el derecho a la libertad de circulación, que se esclarece en la observación general Nº 27[15]. Las limitaciones que se enuncian en la observación incluyen, entre otras cosas, los elementos que se consignan a continuación:

a) Todas las restricciones deben ser previstas por la ley (párrs. 11 y 12);

b) Las restricciones no deben comprometer la esencia de un derecho humano (párr. 13);

c) Las restricciones deben ser necesarias en una sociedad democrática (párr. 11);

d) La aplicación de restricciones no debe conferir una discrecionalidad sin trabas (párr. 13);

e) No basta con que las restricciones se utilicen para conseguir uno de los fines permisibles enumerados; deben ser necesarias también para conseguir el objetivo legítimo. (párr. 14);

f) Las medidas restrictivas deben ajustarse al principio de proporcionalidad; deben ser adecuadas para desempeñar su función protectora; debe ser el instrumento menos perturbador de los que permitan conseguir el resultado deseado, y deben guardar proporción con el interés que debe protegerse (párrs. 14 y 15).

C. Consideraciones recientes de mecanismos internacionales para la protección de los derechos humanos

30. En informes anteriores, el Relator Especial evaluó la repercusión de Internet en la realización del derecho a la libertad de opinión y expresión (A/HRC/17/27 y A/66/290). Observó que, aunque los usuarios podían disfrutar en Internet de un anonimato relativo, los Estados y agentes privados también tenían acceso a nuevas tecnologías de seguimiento y reunión de información sobre las comunicaciones y actividades de estos usuarios. Esas tecnologías podían constituir una violación del derecho de los usuarios a la intimidad y, al socavar la confianza del público y la seguridad de Internet, obstruir el libre flujo de información e ideas en línea. El Relator Especial instó a los Estados a adoptar leyes eficaces de protección de la intimidad y los datos de conformidad con las normas de derechos humanos y a adoptar todas las medidas apropiadas por que las personas pudieran expresarse anónimamente en línea[16].

31. Otros titulares de mandatos de procedimientos especiales examinaron la cuestión de la injerencia en el derecho a la intimidad. El Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo examinó la evolución de las prácticas y las tecnologías de vigilancia que han afectado adversamente al derecho a la intimidad usando como justificación la lucha contra el terrorismo[17]. El Relator Especial subrayó que estas medidas no solo habían conducido a

[14] *Ibid.*
[15] Véase también la observación general Nº 34 del Comité de Derechos Humanos.
[16] A/HRC/17/27, pág. 23.
[17] A/HRC/13/37.

violaciones del derecho a la intimidad sino que también habían influido en los derechos a las debidas garantías procesales y en la libertad de circulación, la libertad de asociación y la libertad de expresión. Instó a los gobiernos a que explicaran detalladamente cómo sus políticas de vigilancia se ajustaban a los principios de proporcionalidad y necesidad, de conformidad con las normas internacionales de derechos humanos y qué medidas habían tomado para prevenir abusos. El Relator Especial también insistió en la necesidad de que se aprobaran leyes generales de protección de datos y de la intimidad, y de que se establecieran órganos de supervisión estrictos e independientes facultados para examinar el uso de técnicas de vigilancia invasivas y el procesamiento de la información personal. Además, recomendó que se dedicaran recursos de investigación y desarrollo a tecnologías de promoción de la intimidad.

32. Otros mecanismos de protección de los derechos humanos también han prestado atención recientemente a las consecuencias de la vigilancia de las comunicaciones en la protección de los derechos a la intimidad y la libertad de expresión. Así pues, el Comité de Derechos Humanos expresó su preocupación por las denuncias en el sentido de que el Estado vigilaba el uso de Internet y había bloqueado el acceso a algunos sitios web[18] y recomendó el examen de la legislación que ofrecía al poder ejecutivo amplias facultades de vigilancia en relación con las comunicaciones electrónicas[19]. El Examen Periódico Universal también ha incluido recomendaciones para velar, por ejemplo, por que la legislación relativa a Internet y otras nuevas tecnologías de comunicación respeten las obligaciones internacionales de derechos humanos[20].

V. Modalidades de vigilancia de las comunicaciones

33. Las tecnologías y disposiciones de vigilancia modernos que permiten a los Estados injerirse en la vida privada de las personas atentan contra una diferenciación clara entre el ámbito público y el privado. Facilitan la vigilancia invasiva y arbitraria de las personas, que podrían ni siquiera saber que han sido objeto de esta vigilancia, y menos aún cuestionarla. Los adelantos tecnológicos determinan que la eficacia del Estado para llevar a cabo la vigilancia ya no se vea limitada en función de la escala o la duración. Los menores costos de la tecnología y el almacenamiento de datos han permitido eliminar los desincentivos financieros o prácticos de realizar la vigilancia. En consecuencia, ahora el Estado tiene mayor capacidad que nunca para emprender una vigilancia simultánea, invasiva, selectiva y de escala amplia.

A. Vigilancia selectiva de las comunicaciones

34. Los Estados tienen acceso a diversas técnicas y tecnologías para llevar a cabo la vigilancia de las comunicaciones privadas de las personas seleccionadas. La capacidad de interceptación en tiempo real permite a los Estados escuchar y grabar las llamadas telefónicas de cualquier persona que utiliza un teléfono fijo o móvil mediante medios de interceptación para la vigilancia estatal que todas las redes de comunicaciones deben incorporar en sus sistemas[21]. Puede establecerse la ubicación de una persona y leerse y grabarse sus mensajes de texto. Mediante la colocación de un dispositivo en un cable de

[18] CCPR/C/IRN/CO/3.
[19] CCPR/C/SWE/CO/6.
[20] A/HRC/14/10.
[21] Véanse, por ejemplo, la Ley de Asistencia en Materia de Comunicaciones para la Aplicación de la Ley de 1994 (Estados Unidos); la Ley de Telecomunicaciones de 1997, Parte 15 (Australia); la Ley de Regulación de las Atribuciones de Investigación de 2000, arts.12 a 14 (Reino Unido); y la Ley de Telecomunicaciones (Capacidad de Interceptación) de 2004.

Internet vinculado a un lugar o una persona determinados, las autoridades estatales también pueden vigilar la actividad en línea de esa persona, incluidos los sitios web que consulta.

35. El acceso al contenido almacenado de los correos electrónicos y los mensajes de una persona, además de otros datos relacionados con las comunicaciones, pueden obtenerse por conducto de las empresas y los proveedores de servicios de Internet. La iniciativa del organismo europeo de establecimiento de normas, el Instituto Europeo de Normas de Telecomunicaciones, de obligar a los proveedores de servicios en nube[22] a que incorporen "capacidad de interceptación legítima" en la tecnología en nube para permitir a las autoridades estatales tener acceso directo al contenido almacenado por estos proveedores, incluidos correos electrónicos, mensajes y mensajes de voz, es motivo de preocupación[23].

36. Los Estados pueden seguir los movimientos de teléfonos móviles específicos, detectar a todas las personas que tienen teléfonos móviles en una zona determinada e interceptar las llamadas y los mensajes de texto por medio de distintos métodos. Algunos Estados usan dispositivos para la vigilancia de teléfonos móviles apagados denominados receptores del número de Identificación Internacional de Abonados Móviles (IMSI), que pueden instalarse temporalmente en un lugar (como una manifestación o marcha) o permanentemente (como un aeropuerto u otros puestos fronterizos). Estos receptores imitan la torre de telefonía móvil enviando y respondiendo señales de teléfonos móviles a fin de extraer el número de tarjeta SIM (módulo de identidad del abonado) de todos los teléfonos móviles de un territorio determinado.

37. Los Estados están adquiriendo cada vez más programas informáticos que pueden utilizarse para infiltrarse en una computadora personal, un teléfono móvil u otro dispositivo digital[24]. Los programas informáticos de interceptación maliciosa, incluidos los llamados "troyanos" (también conocidos como programas espía *(spyware)* o programas dañinos *(malwarwe)*), pueden utilizarse para encender el micrófono o la cámara de un dispositivo, rastrear la actividad del dispositivo y acceder a información almacenada en el dispositivo, modificarla o borrarla. Estos programas permiten a un Estado ejercer el control absoluto del dispositivo infiltrado, y son prácticamente imposibles de detectar.

B. Vigilancia de las comunicaciones a gran escala

38. Los costos y obstáculos logísticos de realizar una vigilancia a gran escala siguen disminuyendo rápidamente, al tiempo que proliferan las tecnologías que permiten una interceptación, vigilancia y análisis amplios de las comunicaciones. Actualmente, algunos Estados tienen capacidad para rastrear y grabar las comunicaciones telefónicas y de Internet a escala nacional. Al intervenir los cables de fibra óptica por los que se transmite la mayoría de las comunicaciones digitales y aplicar técnicas de reconocimiento de palabras, voz y habla, los Estados pueden lograr el control prácticamente absoluto de las telecomunicaciones y las comunicaciones a través de Internet. Presuntamente estos sistemas fueron adoptados por los Gobiernos de Egipto y Libia en el período anterior a la Primavera Árabe[25].

[22] Un proveedor de servicios en nube ofrece el almacenamiento en línea de datos de redes.

[23] Instituto Europeo de Normas de Telecomunicaciones, DTR 101 567 VO.0.5 (2012-14), *Draft Technical Report: Lawful Interception (LI)*; *Cloud/Virtual Services (CLI)*.

[24] Toby Mendel, Andrew Puddephatt, Ben Wagner, Dixi Hawtin, y Natalia Torres, "Global Survey on Internet Privacy and Freedom of Expression", *UNESCO Series on Internet Freedom* (2012), pág. 41.

[25] Parlamento Europeo, Departamento de Políticas de la Dirección General de Políticas Exteriores, *After the Arab Spring: New Paths for Human Rights and the Internet in European Foreign Policy* (2012), págs. 9 y 10.

39. En muchos Estados la conservación obligatoria de datos está facilitando la recopilación a gran escala de datos que luego pueden refinarse y analizarse. Las tecnologías permiten a los Estados fiscalizar llamadas telefónicas y mensajes de texto para detectar el uso de determinadas palabras, voces o frases, o filtrar la actividad en Internet para saber cuándo una persona consulta ciertos sitios web o accede a determinados recursos en línea. Pueden designarse "cajas negras" para inspeccionar los datos que fluyen a través de Internet y filtrarlos para deconstruir toda la información acerca de la actividad en línea. Este método, llamado "inspección de paquetes profunda", permite al Estado ir más allá de la simple adquisición de conocimientos acerca de los sitios que las personas consultan, y analizar el contenido de los sitios web consultados. Así pues, presuntamente los Estados que se enfrentaron con los levantamientos populares recientes en el Oriente Medio y la región de África Septentrional utilizaron la "inspección de paquetes profunda"[26].

40. Otra herramienta utilizada regularmente por los Estados en la actualidad es la vigilancia de las redes sociales. Los Estados tienen la capacidad para vigilar físicamente las actividades de los sitios de redes sociales, *blogs* y medios de comunicación para establecer conexiones y relaciones, opiniones y asociaciones, y hasta ubicaciones. Además, los Estados pueden aplicar tecnologías sumamente complejas de extracción de datos a la información a disposición del público o a los datos de las comunicaciones proporcionados por terceras partes proveedoras de servicios. En un nivel más básico, los Estados han adquirido medios técnicos para obtener los nombres de usuarios y las contraseñas de sitios de redes sociales como Facebook[27].

C. Acceso a datos de las comunicaciones

41. Además de interceptar y rastrear el contenido de las comunicaciones de personas, los Estados también pueden procurar el acceso a datos de las comunicaciones de terceras partes proveedoras de servicios y empresas de Internet. A medida que el sector privado recopila gradualmente un mayor volumen de distintos datos que revelan información de carácter confidencial acerca de la vida cotidiana de las personas, y los particulares y empresas almacenan el contenido de sus comunicaciones, como mensajes de voz, correos electrónicos y documentos, en los equipos de terceras partes proveedoras de servicios, el acceso a los datos de las comunicaciones se convierte en una técnica de vigilancia cada vez más valiosa empleada por los Estados.

42. El Estado puede utilizar los datos de las comunicaciones reunidos por terceras partes proveedoras de servicios, incluidas grandes empresas de Internet, para componer un perfil completo de las personas de que se trata. Mediante el acceso a estos y su análisis, hasta los registros de transacciones aparentemente inocuas sobre comunicaciones pueden en forma colectiva generar un perfil de la vida privada de la persona, entre otras cosas su estado de salud, sus opiniones o afiliación políticas y religiosas, sus interacciones e intereses, y revelar tantos datos como los que se desprenderían del contenido de las comunicaciones únicamente, o incluso más[28]. Al combinar la información sobre relaciones, ubicación, identidad y actividad, los Estados pueden rastrear el movimiento de las personas y sus actividades en una amplia variedad de ámbitos, desde los lugares a los que viajan hasta dónde estudian, qué leen o con quién interactúan.

43. Los casos de acceso a los datos de las comunicaciones por los Estados están aumentando rápidamente. En los tres años desde que Google presenta informes sobre el

[26] Mendel y otros, *op. cit.*, pág. 43.

[27] Parlamento Europeo, *op. cit.*, pág. 6.

[28] Alberto Escudero Pascual y Gus Hosein, "Questioning lawful access to traffic data", *Communications of the ACM*, vol. 47, Nº 3, marzo de 2004, págs. 77 a 82.

número de solicitudes de datos de las comunicaciones que recibe, estas solicitudes prácticamente se han duplicado, de 12.539 en el último semestre de 2009, a 21.389 en el último semestre de 2012[29]. En el Reino Unido, donde las fuerzas del orden están facultadas para autorizar sus propias solicitudes de información sobre comunicaciones, se registraron 500.000 de estas solicitudes por año[30]. En la República de Corea, un país de casi 50 millones de personas, se presentan unos 37 millones de solicitudes de datos de las comunicaciones por año[31].

D. Filtrado de la información contenida en Internet y censura

44. Los adelantos tecnológicos no solo han facilitado la interceptación de las comunicaciones y el acceso a estas en casos concretos sino que también han permitido a los Estados filtrar la actividad en línea en forma generalizada, incluso a nivel nacional. En muchos países, el filtrado de la información contenida en Internet se lleva a cabo con el pretexto de mantener la armonía social o de erradicar la expresión del odio, aunque lo cierto es que se usa para eliminar el disenso, la crítica o el activismo.

45. Las tecnologías para filtrar información contenida en Internet que se mencionan más arriba también facilitan la vigilancia de la actividad en la Web a fin de permitir al Estado detectar imágenes, direcciones de sitios web u otros contenidos prohibidos, y censurarlos o modificarlos. Los Estados pueden usar estas tecnologías para detectar el empleo de palabras o frases específicas y censurarlas o reglamentar su uso, o establecer quiénes las usan. En países con niveles elevados de penetración de Internet, el filtrado de la información contenida en Internet presuntamente permite la censura del contenido del sitio web y las comunicaciones y facilita la vigilancia de los defensores y activistas de los derechos humanos[32].

46. Además de las tecnologías que facilitan el filtrado y la censura, muchos Estados están filtrando manualmente la información contenida en Internet, creando fuerzas de policía e inspectores en línea para vigilar físicamente el contenido de los sitios web, las redes sociales, los *blogs* y otros medios de comunicación. En algunos Estados, la "ciberpolicía" se encarga de la inspección y el control de Internet, buscando en sitios web y en nodos críticos dentro de sitios web (especialmente en foros de debate en línea) con miras a bloquear o clausurar sitios web que contienen material que el Gobierno desaprueba, o críticas a los dirigentes del país. La carga de esta actividad recae en los intermediarios privados, como los motores de búsqueda y las plataformas de redes sociales, por medio de leyes que amplían la responsabilidad respecto del contenido prohibido del emisor original a todos los intermediarios.

E. Restricciones al anonimato

47. Uno de los adelantos más importantes facilitado por la aparición de Internet fue la capacidad de acceder a información y de impartirla en forma anónima, así como de comunicarla en forma segura sin tener que revelar la identidad. Inicialmente, esto fue

[29] Véase http://www.google.com/transparencyreport/userdatarequests/.

[30] Véase http://www.intelligencecommissioners.com/docs/0496.pdf.

[31] Money Today, 23 de octubre de 2012, citando la revelación de la Comisión de Comunicaciones de Corea en la auditoría nacional anual a la integrante de la Asamblea Nacional Yoo Seung-Hui, http://www.mt.co.kr/view/mtview.php?type=1&no=2012102309430241764&outlink=1.

[32] Parlamento Europeo, Departamento de Políticas de la Dirección General de Políticas Exteriores, *After the Arab Spring: New Paths for Human Rights and the Internet in European Foreign Policy* (2012), pág. 12.

posible pues Internet no tenía una "capa de identidad"; al principio, no se podía saber quién estaba detrás de una comunicación específica, una dirección de correo electrónico, ni siquiera una computadora determinada. No obstante, en nombre de la seguridad y el orden público, gradualmente los Estados han eliminado las oportunidades de comunicación anónima. En muchos Estados, las personas deben identificarse en los cibercafés y registrar sus transacciones en computadoras públicas. Cada vez más, deben presentarse documentos de identidad y registrarse al comprar una tarjeta SIM o un dispositivo de telefonía móvil, al consultar determinados sitios web importantes, o publicar comentarios en sitios web o *blogs*.

48. Las restricciones al anonimato facilitan la vigilancia de las comunicaciones por el Estado al simplificar la detección de las personas que acceden a contenidos prohibidos o los divulgan, y tornan a estas personas más vulnerables a otras formas de vigilancia del Estado.

49. En este sentido, las restricciones al anonimato tienen un efecto disuasorio, desalentando la libre expresión de información e ideas. También pueden dar lugar a la exclusión efectiva de las personas de ámbitos sociales vitales, socavando sus derechos a la expresión y la información y exacerbando las desigualdades sociales. Además, las restricciones al anonimato facilitan la reunión y recopilación de un gran volumen de datos por el sector privado, imponiendo una pesada carga y responsabilidad en los agentes empresariales que deben proteger la confidencialidad y seguridad de dichos datos.

VI. Preocupaciones relativas a las normas jurídicas nacionales

50. En general, la legislación no ha seguido el ritmo de los cambios tecnológicos. En la mayoría de los Estados, las normas jurídicas o bien no existen o son insuficientes para responder al entorno moderno de vigilancia de las comunicaciones. En consecuencia, los Estados están procurando cada vez más justificar el uso de nuevas tecnologías en el ámbito de los antiguos marcos jurídicos, sin reconocer que las capacidades ampliadas que ahora poseen trascienden considerablemente lo previsto en esos marcos. En muchos países, esto significa que se están invocando disposiciones jurídicas imprecisas y de carácter general para legitimar y sancionar el uso de técnicas sumamente invasivas. Sin leyes explícitas que autoricen estas tecnologías y técnicas, y que definan el alcance de su uso, las personas no podrán prever, ni siquiera conocer, su aplicación. Al mismo tiempo, se están aprobando leyes para ampliar la magnitud de las excepciones en materia de seguridad nacional, que prevén la legitimación de técnicas de vigilancia invasivas sin supervisión ni examen independiente alguno.

51. Las normas jurídicas insuficientes incrementan el riesgo de que se vulneren los derechos humanos de las personas, incluidos el derecho a la intimidad y el derecho a la libertad de expresión. También tienen un efecto adverso en determinados grupos de personas, por ejemplo, miembros de algunos partidos políticos, sindicalistas o minorías nacionales, étnicas y lingüísticas, que podrían ser más vulnerables a la vigilancia de las comunicaciones por el Estado. Sin protecciones jurídicas sólidas, los periodistas, los defensores de los derechos humanos y los activistas políticos corren el riesgo de ser objeto de actividades de vigilancia arbitrarias.

52. La vigilancia de los defensores de los derechos humanos en muchos países ha sido bien documentada. En estos casos, los defensores de los derechos humanos y los activistas políticos denuncian que se vigilan sus llamadas telefónicas y sus correos electrónicos, y se rastrean sus movimientos. Los periodistas también son especialmente vulnerables a que se vigilen sus comunicaciones debido a su dependencia de la comunicación en línea. A fin de recibir y hacer el seguimiento de información de fuentes confidenciales, incluidos los

denunciantes de irregularidades, los periodistas deben estar en condiciones de contar con comunicaciones privadas, seguras y anónimas. Un entorno en que la vigilancia está generalizada y no está restringida por las debidas garantías procesales ni la supervisión judicial es incompatible con la protección de las fuentes. Incluso el uso ejecutivo limitado, no transparente y no documentado de la vigilancia puede tener un efecto disuasorio sin la documentación cuidadosa y pública de su uso, y mecanismos de control conocidos para prevenir su uso abusivo.

53. En las subsecciones que figuran a continuación se consignan las preocupaciones comunes relativas al control estatal de la vigilancia de las comunicaciones en circunstancias que atentan contra los derechos a la libertad de expresión y la intimidad.

A. Ausencia de supervisión judicial

54. Mientras que tradicionalmente se exigía que la vigilancia de las comunicaciones estuviese autorizada por el poder judicial, este requisito se está reduciendo o eliminando cada vez más. En algunos países, la interceptación de las comunicaciones puede ser autorizada por un ministro gubernamental, su representante, o un comité. En el Reino Unido, por ejemplo, el Secretario de Estado[33] autoriza la interceptación de las comunicaciones; en Zimbabwe, lo hace el Ministro de Transporte y Comunicaciones[34]. Gradualmente, la vigilancia de las comunicaciones también puede autorizarse en forma amplia e indiscriminada, sin necesidad de que las autoridades encargadas de hacer cumplir la ley establezcan el fundamento para la vigilancia atendiendo a cada caso.

55. Muchos Estados han eliminado el requisito de que los organismos encargados de hacer cumplir la ley vuelvan a presentarse ante el tribunal para mantener la supervisión una vez que se ha emitido una orden de interceptación. Con arreglo a la Ley de Prevención del Terrorismo de Kenya de 2012, por ejemplo, la interceptación de las comunicaciones puede llevarse a cabo en forma indefinida, sin que sea necesario que los organismos encargados de hacer cumplir la ley informen a un tribunal o soliciten una prórroga. Algunos Estados establecen plazos para la ejecución de las órdenes de interceptación pero permiten a las autoridades encargadas de hacer cumplir la ley renovar dichas órdenes en forma reiterada e indefinida.

56. Aun en los casos en que la ley exige autorización judicial, muchas veces en la práctica se trata de una aprobación arbitraria de solicitudes de aplicación de la ley. En particular esto sucede cuando los requisitos establecidos por las autoridades encargadas de hacer cumplir la ley son escasos. Así pues, la Ley de 2010 de Regulación de la Interceptación de las Comunicaciones de Uganda solo requiere que las autoridades encargadas de hacer cumplir la ley demuestren que hay motivos "razonables" para permitir que se realice la interceptación. En esos casos, la carga de la prueba para establecer la necesidad de vigilancia es sumamente reducida, habida cuenta del potencial de la vigilancia de dar lugar a investigaciones, discriminación o vulneración de los derechos humanos. En otros países, un conjunto complejo de leyes autoriza el acceso a las comunicaciones y la vigilancia de estas en virtud de diferentes circunstancias. En Indonesia, por ejemplo, la Ley de Sustancias Sicotrópicas, la Ley de Estupefacientes, la Ley sobre Información y Transacciones Electrónicas, la Ley de Telecomunicaciones y la Ley contra la Corrupción contienen elementos sobre la vigilancia de las comunicaciones. En el Reino Unido, más de 200 organismos, fuerzas policiales y autoridades penitenciarias están autorizados a adquirir datos de comunicaciones en virtud de la Ley de Regulación de Facultades de

[33] Artículo 5 de la Ley de Regulación de Facultades de Investigación de 2000.
[34] Artículo 5 de la Ley de Interceptación de las Comunicaciones de 2006.

Investigación de 2000. En consecuencia, es difícil que los particulares puedan prever cuándo podrían ser objeto de vigilancia o qué organismo del Estado se encargaría de ello.

57. En muchos Estados los proveedores de servicios de comunicaciones se ven obligados a modificar su infraestructura para permitir la vigilancia directa, eliminando así la posibilidad de supervisión judicial. Así pues, en 2012 el Ministerio de Justicia y el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia emitieron un decreto por el cual dispusieron que los proveedores de servicios de telecomunicaciones tenían la obligación de establecer infraestructura que permitiese acceso directo a las comunicaciones a la Policía Judicial, sin la autorización previa del Fiscal General de la Nación[35]. La Ley de 2010 de Regulación de la Interceptación de las Comunicaciones de Uganda (art. 3) mencionada dispone el establecimiento de un centro de vigilancia y mandatos en el sentido de que los proveedores de servicios de telecomunicaciones garanticen que las comunicaciones interceptadas se transmitan al centro de vigilancia (art. 8 1) f)). El Gobierno de la India ha propuesto la instalación de un Sistema de Vigilancia Centralizado que distribuirá todas las comunicaciones al Gobierno central, lo que permitirá a los organismos de seguridad evitar la interacción con el proveedor de servicios[36]. Estas disposiciones permiten que la vigilancia de las comunicaciones se lleve a cabo sin autorización judicial y que sea secreta y no regulada, eliminando toda transparencia y rendición de cuentas por parte del Estado.

B. Excepciones en función de la seguridad nacional

58. Las nociones imprecisas y no especificadas de "seguridad nacional" se han convertido en una justificación aceptable para la interceptación de las comunicaciones en muchos países y el acceso a estas. Así pues, en la India, la Ley de Tecnología de la Información de 2008 permite la interceptación de las comunicaciones, entre otras cosas, en aras de "la soberanía, la integridad o la defensa de la India, las relaciones amistosas con Estados extranjeros, el orden público y la investigación de todo delito" (art. 69).

59. En muchos casos, los organismos nacionales de inteligencia también gozan de excepciones generales al requisito de la autorización judicial. Así pues, la Ley de Vigilancia de Inteligencia Extranjera de los Estados Unidos empodera al Organismo Nacional de Seguridad a interceptar comunicaciones sin autorización judicial cuando una parte en la comunicación se encuentra fuera de los Estados Unidos y hay motivos razonables para creer que un participante es miembro de una organización terrorista identificada por el Estado. La legislación de Alemania permite escuchas telefónicas automáticas sin autorización judicial de comunicaciones nacionales e internacionales por los servicios de inteligencia estatales a los efectos de proteger el orden democrático libre, la existencia o la seguridad del Estado[37]. En Suecia, la Ley sobre Interceptación de Señales en Operaciones de Defensa autoriza al organismo sueco de inteligencia a interceptar sin una autorización judicial u orden de los tribunales todas las comunicaciones telefónicas o a través de Internet que se llevan a cabo dentro de las fronteras de Suecia. En la República Unida de Tanzanía, la Ley del Servicio de Inteligencia y Seguridad de 1996 permite a los servicios de inteligencia nacionales llevar a cabo investigaciones relativas a cualquier persona u organismo si tienen una causa razonable para considerarla un riesgo, una fuente de riesgo o una amenaza para la seguridad del Estado.

[35] Decreto Nº 1704 del Ministerio de Justicia y del Ministerio de Tecnologías de la Información y las Comunicaciones. Basado en el Código de Procedimiento Penal de 2004.

[36] Departamento of Comunicaciones del Gobierno de la India. *Annual Report 2011-2012*, pág. 58; http://www.dot.gov.in/annualreport/AR%20Englsih%2011-12.pdf.

[37] Ley Nº G-10.

60. El uso de un concepto impreciso de seguridad nacional para justificar limitaciones invasivas del goce de los derechos humanos plantea serias preocupaciones[38]. Este concepto tiene una definición amplia y, por consiguiente, es vulnerable a la manipulación del Estado como medio de justificar medidas dirigidas a grupos vulnerables como defensores de los derechos humanos, periodistas o activistas. También permite justificar el secreto a menudo innecesario en torno a investigaciones o actividades de las fuerzas del orden, socavando los principios de la transparencia y la rendición de cuentas.

C. Acceso no regulado a datos de las comunicaciones

61. El acceso a datos de las comunicaciones en poder de proveedores de servicios de comunicaciones nacionales suele regirse por la legislación o por las condiciones previstas en las licencias. En consecuencia, por lo general los Estados tienen acceso irrestricto a los datos de las comunicaciones con escasa supervisión o reglamentación. Así pues, en virtud de una ley del Brasil sobre el lavado de dinero se otorga a la policía y a los proveedores de servicios de comunicaciones acceso a información registrada en Internet sin una orden judicial[39]. A nivel internacional, la provisión de acceso a datos de las comunicaciones se regula por medio de tratados bilaterales de asistencia judicial recíproca. No obstante, esta cooperación suele establecerse fuera del ámbito de la ley sobre la base del cumplimiento voluntario del proveedor del servicio o la empresa de Internet. Así pues, el acceso a los datos de las comunicaciones puede obtenerse en muchos Estados sin autorización independiente y con supervisión limitada.

D. Vigilancia fuera del marco jurídico

62. Algunos medios de vigilancia mencionados anteriormente recaen fuera de los marcos jurídicos vigentes, aunque han sido adoptados en forma generalizada por los Estados. Los programas informáticos ilegales invasivos como los troyanos o los mecanismos de interceptación a gran escala atentan seriamente contra las nociones tradicionales de vigilancia que no pueden conciliarse con la legislación en vigor sobre vigilancia ni con el acceso a la información privada. No se trata simplemente de nuevos métodos para llevar a cabo la vigilancia, sino de nuevas formas de vigilancia. Desde la perspectiva de los derechos humanos, el uso de estas tecnologías es sumamente perturbador. Por ejemplo, los troyanos no solo permiten al Estado acceder a dispositivos, sino que también les permiten modificar, en forma inadvertida o deliberada, la información allí contenida. Esto atenta no solo contra el derecho a la intimidad y los derechos a la equidad procesal respecto del uso de estas pruebas en las actuaciones judiciales. La tecnología de interceptación a gran escala menoscaba toda consideración de proporcionalidad al facilitar la vigilancia indiscriminada. Permite al Estado copiar y vigilar todos los actos de comunicación en un país o zona determinados, sin obtener autorización para los casos individuales de interceptación.

63. A menudo los gobiernos no reconocen el uso de estas tecnologías para llevar a cabo la vigilancia, o sostienen que estas tecnologías se están empleando legítimamente en el marco de la legislación sobre vigilancia en vigor. Aunque está claro que muchos Estados poseen programas informáticos que permiten la interceptación ilegal, como la tecnología de troyanos, su fundamento jurídico no se ha debatido públicamente en ningún Estado, con excepción de Alemania. En ese contexto, en 2006 la provincia de Renania del Norte-

[38] Resoluciones del Consejo de Derechos Humanos sobre la lucha contra el terrorismo.

[39] Ley Federal del Brasil Nº 12683/2012, art. 17-B. Puede consultarse en: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12683.htm.

Westfalia promulgó legislación por la que autorizó el "acceso secreto a un sistema de tecnología de la información" (artículo 5.2, Nº 11, de la Ley de Protección Constitucional de Renania del Norte-Westfalia), que se consideró una infiltración técnica por medio de la instalación de un programa espía o el aprovechamiento de lagunas de seguridad del sistema. El Tribunal Constitucional Federal de Alemania derogó la Ley en febrero de 2008 y dictaminó que estas medidas solo estarían en consonancia con los derechos humanos si se sometían a autorización y examen judiciales, y se aplicaban únicamente en los casos en que podría correrse un peligro concreto en relación con un interés jurídico de importancia fundamental[40].

E. Aplicación extraterritorial de las leyes de vigilancia

64. En respuesta al aumento de los flujos de datos a través de las fronteras y al hecho de que la mayoría de las comunicaciones son almacenadas por terceras partes extranjeras que proveen servicios, algunos Estados han comenzado a aprobar leyes que tienen por objeto autorizarlas a llevar a cabo la vigilancia extraterritorial o a interceptar las comunicaciones en jurisdicciones extranjeras. Esto plantea una grave preocupación respecto de la comisión extraterritorial de violaciones de los derechos humanos y la incapacidad de las personas de saber si pueden ser objeto de vigilancia extranjera, impugnar decisiones respecto de la vigilancia extranjera o tener recurso a reparaciones. En Sudáfrica, por ejemplo, el proyecto de ley de enmienda de las Leyes Generales de Inteligencia permite la vigilancia de las comunicaciones extranjeras fuera de Sudáfrica o que pasan por el territorio del país[41]. En octubre de 2012, el Ministerio Neerlandés de Justicia y Seguridad propuso algunas enmiendas legislativas al Parlamento que permitirían a la policía acceder a las computadoras y los teléfonos móviles en los Países Bajos y el extranjero para instalar programas espía *(spyware)* y buscar y destruir datos[42]. En diciembre de 2012, la Asamblea Nacional del Pakistán promulgó la Ley de Juicio Justo de 2012, cuyo párrafo 31 dispone la ejecución de órdenes de vigilancia en jurisdicciones extranjeras. Más tarde ese mes, los Estados Unidos renovaron la Ley de Enmienda de Vigilancia de Inteligencia Exterior de 2008 por la que se prorrogó la facultad del Gobierno para realizar actividades de vigilancia de ciudadanos no estadounidenses fuera de los Estados Unidos (art. 1881a), incluidos nacionales extranjeros cuyas comunicaciones están alojadas en servicios en nube en los Estados Unidos (como Google y otras grandes empresas de Internet)[43]. También en 2012, el Instituto Europeo de Normas de Telecomunicaciones redactó proyectos de normas para la interceptación de servicios extranjeros en nube por los Gobiernos europeos[44]. Estos acontecimientos sugieren una tendencia alarmante hacia el otorgamiento de atribuciones de vigilancia fuera de las fronteras territoriales, aumentando el riesgo de acuerdos de cooperación entre las fuerzas del orden del Estado y los organismos de seguridad, que permiten eludir las restricciones jurídicas internas.

[40] Puede consultarse en alemán. BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. (1-67), http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html.

[41] Artículo 1. c. proyecto de ley de enmienda de las Leyes Generales de Inteligencia. Puede consultarse en: http://www.parliament.gov.za/live/commonrepository/Processed/20111201/385713_1.pdf.

[42] Véase http://www.edri.org/edrigram/number10.20/dutch-proposal-state-spyware.

[43] Véase Parlamento Europeo, Dirección General de Políticas Interiores, Departamento Temático C: Derechos de los Ciudadanos y Asuntos Constitucionales, *Fighting crime and protecting privacy in the cloud,* estudio, 2012.

[44] Borrador del Instituto Europeo de Normas de Telecomunicaciones DTR 101 567 *Lawful Interception (LI)* vol.1.0 (2012-05); *Cloud/Virtual Services (CLI)*. Puede consultarse en: www.3gpp.org.

F. Conservación obligatoria de datos

65. A fin de aumentar el almacenamiento de los datos de comunicaciones a los que pueden acceder, algunos Estados están aprobando leyes sobre la conservación obligatoria de datos por las que exigen a los proveedores de servicios de Internet y de telecomunicaciones (colectivamente denominados "proveedores de servicios de comunicaciones") reunir y conservar en forma permanente el contenido de las comunicaciones y la información acerca de las actividades en línea de los usuarios. Estas leyes permiten la recopilación de registros históricos sobre los correos electrónicos y los mensajes de las personas, así como la ubicación y la interacción con amigos y familiares, entre otras cosas.

66. Al prestar servicios a sus usuarios, los proveedores de servicios de comunicaciones dan a los abonados dispositivos o les asignan una dirección de Protocolo de Internet (IP)[45] que cambia periódicamente. La información sobre una dirección IP puede utilizarse para determinar la identidad y ubicación de una persona y seguir su actividad en línea. Las leyes de conservación obligatoria de datos imponen a los proveedores de servicios de comunicaciones la obligación de conservar los registros de sus asignaciones de direcciones IP durante cierto período, lo que da al Estado mayor capacidad para exigir a los proveedores de servicios de comunicaciones que indiquen la identidad de una persona en función de la dirección de IP que tenía en un momento y lugar determinados. Actualmente algunos Estados también están procurando obligar a las terceras partes proveedoras de servicios a que reúnan y conserven información que normalmente no reunirían.

67. Las leyes nacionales de conservación de datos son invasivas y costosas, y atentan contra los derechos a la intimidad y la libre expresión. Al obligar a los proveedores de servicios de comunicaciones a generar grandes bases de datos acerca de quién se comunica con quién telefónicamente o por Internet, la duración del intercambio y la ubicación de los usuarios, y a guardar esta información (a veces durante varios años), las leyes de conservación obligatoria de datos aumentan considerablemente el alcance de la vigilancia del Estado, y de este modo el alcance de las violaciones de los derechos humanos. Las bases de datos de comunicaciones se vuelven vulnerables al robo, el fraude y la revelación accidental.

G. Leyes sobre la revelación de la identidad

68. En muchos Estados, las leyes exigen la presentación de documentos de identidad en los cibercafés. Estas leyes son especialmente problemáticas en particular en los países en que la propiedad de computadoras personales es escasa y las personas utilizan principalmente computadoras públicas. En la India, por ejemplo, las Normas de Tecnología de la Información (Directrices para Cibercafés) de 2011, disponen que los propietarios de cibercafés exijan la presentación de documentos de identidad de todas las personas que visitan el cibercafé, que debe conservar sus registros por lo menos durante un año (Norma 4 2)). El cibercafé debe mantener un registro que incluya, entre otras cosas, la hora de comienzo y de cese de la comunicación, y la identificación de la computadora durante por lo menos un año (Norma 5 1) y 5 2)); y almacenar y conservar copias de respaldo de todos los registros de acceso o entrada de comunicación de los usuarios durante por lo menos un año (Norma 5 4)).

69. Ahora los particulares también tienen la obligación de usar sus nombres verdaderos en línea en muchos Estados, y de establecer su identidad en forma oficial. En la República

[45] Una dirección IP es un código numérico único que identifica a todas las computadoras u otros dispositivos conectados a Internet.

de Corea, la Ley de Información sobre Comunicaciones, aprobada en 2007, exige que los usuarios registren su nombre verdadero antes de acceder a los sitios web de más de 100.000 consultas diarias, aparentemente para reducir la intimidación y la expresión del odio en línea. Recientemente el Tribunal Constitucional rechazó la Ley por considerar que restringía la libertad de palabra y socavaba la democracia[46]. Hace poco China adoptó la Decisión sobre el Fortalecimiento de la Protección de la Información en Línea, que exige que los proveedores de telecomunicaciones y servicios de Internet reúnan información personal acerca de los usuarios que solicitan acceso a Internet, así como servicios de telefonía fija o móvil. Los proveedores de servicios que permiten a los usuarios publicar en línea tienen la obligación de vincular los nombres de los usuarios con su verdadera identidad. El requisito del nombre verdadero permite a las autoridades establecer con más facilidad la identidad de los autores de los comentarios en línea o vincular los dispositivos móviles con determinadas personas, eliminando así las expresiones anónimas[47].

70. Otra iniciativa que impide el anonimato de las comunicaciones es la adopción gradual de políticas que requieren el registro de tarjetas SIM con el nombre verdadero del abonado o un documento de identidad emitido por el Gobierno. En 48 países de África las leyes que exigen la inscripción de datos personales en el registro del proveedor de servicios de red para obtener la activación de tarjetas SIM prepagas aparentemente están facilitando el establecimiento de bases de datos amplias de información sobre los usuarios, eliminando la posibilidad del anonimato en las comunicaciones, posibilitando el rastreo de la ubicación y simplificando la vigilancia de las comunicaciones[48]. En caso de no haber legislación sobre la protección de datos, los departamentos gubernamentales pueden acceder a la información sobre usuarios de tarjetas SIM y esta puede compararse con la contenida en otras bases de datos públicas y privadas, lo que permite al Estado crear perfiles integrales de los ciudadanos. Estos también corren el riesgo de quedar excluidos del uso de servicios de telefonía móvil (que permiten no solo las comunicaciones sino también el acceso a los servicios financieros) en caso de no poder, o no querer, proveer sus datos personales para registrarse.

H. Restricciones al cifrado y principales leyes de revelación de información

71. La seguridad y el anonimato de las comunicaciones también se ven menoscabados por leyes que limitan el uso de herramientas que fomentan la privacidad que pueden utilizarse para proteger las comunicaciones, como el cifrado. Muchos Estados han adoptado leyes que disponen que una persona debe permitir el descifrado cuando se le ordena. La de la Interceptación de Comunicaciones y Disposiciones en materia de Información relativa a las Comunicaciones de 2002 de Sudáfrica exige la asistencia para el descifrado a toda persona que posea la clave de cifrado[49]. En Finlandia (artículo 4 4) a) de la Ley de Medidas Coercitivas Nº 1987/450), en Bélgica (artículo 9 de la Ley sobre Delitos Informáticos de 28

[46] Decisión del Tribunal Constitucional 2010Hun-Ma47 (decisión sobre "nombres verdaderos"), 23 de agosto de 2012. Puede consultarse un resumen oficial de la decisión del Tribunal en el sitio web de este http://www.ccourt.go.kr/home/bpm/sentence01_list.jsp (únicamente en coreano).

[47] "China to Strengthen Internet Information Protection" (China prevé el fortalecimiento de la protección de información en Internet) http://www.ebeijing.gov.cn/BeijingInformation/BeijingNewsUpdate/t1292298.htm.

[48] Kevin P. Donovan y Aaron K. Martin, "The Rise of African SIM Registration: Mobility, Identity, Surveillance and Resistance", *Information Systems and Innovation Group Working Paper Series*, no. 186, London School of Economics and Political Science (2012).

[49] Artículo 29 de la Ley de Reglamentación de la Interceptación de Comunicaciones y Disposiciones en materia de Información relativa a las Comunicaciones de 2002 de Sudáfrica. Puede consultarse en: http://www.dac.gov.za/acts/Regulation%20of%20Interception%20of%20Communications%20Act.pdf.

de noviembre de 2000), y en Australia (artículos 12 y 28 de la Ley sobre Delitos Informáticos de 2001) existe legislación semejante.

VII. Funciones y responsabilidades del sector privado

72. Los adelantos tecnológicos fundamentales que han permitido formas de comunicación nuevas y dinámicas han tenido lugar principalmente en el sector privado. En este sentido, muchos de los cambios en la forma en que comunicamos, recibimos e impartimos información se basan en las investigaciones e innovaciones de los agentes empresariales.

73. El sector privado también ha desempeñado una importante función en cuanto a la facilitación de la vigilancia de las personas de diferentes maneras. Los agentes empresariales han tenido que responder a los requisitos de diseño de las redes digitales y la infraestructura de las comunicaciones a fin de permitir la intervención del Estado. Los Estados adoptaron por primera vez estos requisitos en la década de 1990 y se están volviendo obligatorios para todos los proveedores de servicios de comunicaciones. Cada vez más, los Estados están aprobando legislación que exige a los proveedores de servicios de comunicaciones permitir a los Estados acceso directo a las comunicaciones o modificar infraestructura para facilitar nuevas formas de intervención de los Estados.

74. Al desarrollar y desplegar nuevas tecnologías y herramientas de comunicaciones de formas determinadas, los agentes empresariales también han adoptado voluntariamente medidas que facilitan la vigilancia de las comunicaciones por el Estado. En su manifestación más simple, esta colaboración se ha traducido en decisiones sobre la forma en que los agentes empresariales reúnen y elaboran la información, lo cual les permite convertirse en depositarios en gran escala de información personal que luego se pone a disposición de los Estados, a solicitud de estos. Los agentes empresariales han adoptado especificaciones que permiten el acceso o la intervención del Estado, la reunión de información excesiva o probatoria, o la restricción de la aplicación del cifrado u otras técnicas que podrían limitar el acceso a la información tanto a las empresas como a los gobiernos. Con frecuencia el sector privado no ha provisto tecnología para proteger la intimidad o la ha aplicado de formas poco seguras, que distan de ser las más avanzadas.

75. En los casos más graves, el sector privado ha sido cómplice en el desarrollo de tecnologías que permiten la vigilancia a gran escala o invasiva, en contravención de las normas jurídicas[50]. El sector empresarial ha generado una industria mundial centrada en el intercambio de tecnologías de vigilancia. Estas tecnologías suelen venderse a países en los que hay un riesgo grave de que puedan utilizarse para violar los derechos humanos, en particular los de los defensores de los derechos humanos, los periodistas u otros grupos vulnerables. Esta industria prácticamente no está reglamentada porque los Estados no han seguido el ritmo de la evolución tecnológica y política.

76. Las obligaciones de los Estados en materia de derechos humanos exigen que estos no solo respeten y promuevan los derechos a la libertad de expresión y la intimidad, sino también que protejan a las personas de violaciones de los derechos humanos perpetradas por los agentes empresariales. Además, los Estados deben ejercer una supervisión adecuada con vistas a cumplir sus obligaciones internacionales de derechos humanos cuando contratan los servicios de empresas, o promulgan leyes a tal fin, que puedan tener un

[50] Para algunos ejemplos de tecnología de vigilancia desarrollada por el sector privado y utilizada en Libia, Bahrein, la República Árabe Siria, Egipto y Túnez, véase Parlamento Europeo, Departamento de Políticas de la Dirección General de Políticas Exteriores, *After the Arab Spring: New Paths for Human Rights and the Internet in European Foreign Policy* (2012), págs. 9 y 10.

impacto sobre el disfrute de los derechos humanos[51]. Las obligaciones de derechos humanos en este sentido son aplicables cuando los agentes empresariales operan en el exterior[52].

77. Los Estados deben velar por que el sector privado pueda desempeñar sus funciones de manera independiente y que promueva los derechos humanos de las personas. Al mismo tiempo, no puede permitirse que los agentes empresariales participen en actividades que vulneren los derechos humanos, y los Estados tienen la responsabilidad de hacer que las empresas rindan cuentas en este sentido.

VIII. Conclusiones y recomendaciones

78. **Las técnicas y tecnologías de las comunicaciones han evolucionado considerablemente, cambiando la forma en que los Estados llevan a cabo la vigilancia de las comunicaciones. Por consiguiente, los Estados deben actualizar su comprensión y reglamentación de la vigilancia de las comunicaciones y modificar sus prácticas para velar por el respeto y la protección de los derechos humanos de las personas.**

79. **Los Estados no pueden garantizar que las personas estén en condiciones de buscar y recibir información ni de expresarse a menos que respeten, protejan y promuevan su derecho a la intimidad. La intimidad y la libertad de expresión se relacionan entre sí y son mutuamente dependientes; la vulneración de una de estas puede ser tanto la causa como la consecuencia de la vulneración de la otra. Sin la legislación y las normas jurídicas suficientes que garanticen la intimidad, la seguridad y el anonimato de las comunicaciones, los periodistas, los defensores de los derechos humanos y los denunciantes de irregularidades, por ejemplo, no pueden estar seguros de que sus comunicaciones no serán objeto de control estatal.**

80. **A fin de cumplir sus obligaciones en materia de derechos humanos, los Estados deben velar por que los derechos a la libertad de expresión y la intimidad constituyan la esencia de su marco de vigilancia de las comunicaciones. A tal fin, el Relator Especial recomienda.**

A. Actualizar y fortalecer las leyes y normas jurídicas

81. **La vigilancia de las comunicaciones debe considerarse un acto sumamente perturbador que podría suponer una injerencia en los derechos a la libertad de expresión y la intimidad, y que atenta contra los fundamentos de una sociedad democrática. La legislación debe estipular que la vigilancia de las comunicaciones por el Estado solo se realice en las situaciones más excepcionales y únicamente con la supervisión de una autoridad judicial independiente. La legislación debe incluir salvaguardias relativas a la naturaleza, el alcance y la duración de las posibles medidas, los motivos que se requieren para disponerlas, las autoridades competentes para autorizarlas y supervisarlas, y el tipo de reparaciones previstas en la legislación nacional.**

82. **Las personas deben tener derecho a que se les notifique si han estado sometidas a la vigilancia de las comunicaciones o si el Estado ha accedido a sus datos de comunicaciones. Si bien la notificación por adelantado o simultánea podría atentar contra la eficacia de la vigilancia, debe notificarse a las personas una vez que la**

[51] Principios Rectores sobre las empresas y los derechos humanos: puesta en práctica del marco de las Naciones Unidas para "proteger, respetar y remediar", Principio 5.

[52] Comité de Derechos Humanos, observaciones finales, Alemania, diciembre de 2012.

vigilancia haya finalizado, y darles la posibilidad de obtener reparación por el uso de medidas de vigilancia, con posteridad a ella.

83. **Los marcos jurídicos deben garantizar que las medidas de vigilancia de las comunicaciones:**

a) Estén en consonancia con la ley, cumplan con las normas de claridad y precisión suficientes para que las personas sean notificadas por adelantado y puedan prever su aplicación;

b) Sean estricta y fehacientemente necesarias para lograr un objetivo legítimo; y

c) Se ajusten al principio de proporcionalidad y no se empleen cuando se disponga de técnicas menos invasivas o cuando estas no se hayan agotado.

84. **Los Estados deben penalizar la vigilancia ilegal por los agentes públicos o privados. Estas leyes no deben utilizarse contra denunciantes de irregularidades ni otras personas que desean denunciar violaciones de los derechos humanos, ni deben impedir la legítima vigilancia de la acción gubernamental por los ciudadanos.**

85. **La provisión de datos de las comunicaciones por el sector privado a los Estados debe estar suficientemente reglamentada para garantizar que los derechos humanos de las personas tengan carácter prioritario en todos los casos. Solo debe recurrirse al acceso a los datos de las comunicaciones en poder de los agentes empresariales nacionales en los casos en que se han agotado otras técnicas disponibles menos perturbadoras.**

86. **La provisión de datos de las comunicaciones al Estado debe ser objeto de seguimiento por una autoridad independiente, como un tribunal o un mecanismo de supervisión. A nivel internacional, los Estados deben celebrar tratados de asistencia judicial recíproca que reglamenten el acceso a los datos de las comunicaciones en poder de los agentes empresariales extranjeros.**

87. **Las técnicas y prácticas de vigilancia que se empleen fuera del estado de derecho deben someterse a control legislativo. Su uso extrajudicial socava los principios básicos de la democracia y probablemente tenga efectos políticos y sociales nocivos.**

B. Facilitar comunicaciones privadas, seguras y anónimas

88. **Los Estados deben abstenerse de obligar a los usuarios a presentar sus documentos de identidad como condición previa para obtener acceso a las comunicaciones, incluidos los servicios en línea, los cibercafés o la telefonía móvil.**

89. **Las personas deben tener libertad para usar la tecnología que prefieran para realizar sus comunicaciones. Los Estados no deben injerirse en el uso de tecnologías de cifrado, ni obligar a las personas a proveer claves de cifrado.**

90. **Los Estados no deben conservar ni exigir la retención de información determinada puramente con fines de vigilancia.**

C. Aumentar el acceso público a la información, la comprensión y el conocimiento de las amenazas a la intimidad

91. **Los Estados deben ser completamente transparentes acerca del uso y el alcance de las técnicas y atribuciones de vigilancia de las comunicaciones. Deben publicar,**

como mínimo, información completa sobre el número de solicitudes aprobadas y rechazadas, y un desglose de las solicitudes por proveedor de servicios y por investigación y propósito.

92. **Los Estados deben proporcionar a los particulares información suficiente para permitirles comprender el alcance, la naturaleza y la aplicación de las leyes que permiten la vigilancia de las comunicaciones. Los Estados deben permitir a los proveedores de servicios publicar los procedimientos que aplican cuando abordan la vigilancia de las comunicaciones, seguir esos procedimientos y publicar registros de la vigilancia de las comunicaciones.**

93. **Los Estados deben establecer mecanismos de vigilancia independientes capaces de garantizar la transparencia y la rendición de cuentas de la vigilancia de las comunicaciones por el Estado.**

94. **Los Estados deben aumentar la conciencia pública sobre los usos de las nuevas tecnologías de comunicación para ayudar a las personas a evaluar, gestionar y mitigar los riesgos relativos a las comunicaciones y adoptar decisiones fundamentadas sobre estos.**

D. Reglamentar la comercialización de tecnología de vigilancia

95. **Los Estados deben garantizar que los datos de las comunicaciones reunidos por los agentes empresariales para la provisión de servicios de comunicaciones reúnan las normas más elevadas de protección de datos.**

96. **Los Estados deben abstenerse de obligar al sector privado a aplicar medidas que pongan en riesgo la privacidad, la seguridad y el anonimato de los servicios de comunicaciones, incluidos los que requieren el establecimiento de capacidad de interceptación con fines de vigilancia por el Estado o la prohibición del uso de cifrado.**

97. **Los Estados deben adoptar medidas para prevenir la comercialización de tecnologías de vigilancia, prestando atención especial a la investigación, el desarrollo, el comercio, la exportación y el uso de estas tecnologías teniendo en cuenta su capacidad para facilitar las violaciones sistemáticas de los derechos humanos.**

E. Fomentar la evaluación de las obligaciones pertinentes de derechos humanos

98. **Es muy necesario promover la comprensión internacional de la protección del derecho a la intimidad a la luz de los adelantos tecnológicos. El Comité de Derechos Humanos debe considerar la posibilidad de formular una nueva observación general sobre el derecho a la intimidad, que sustituya a la observación general Nº 16 (1988).**

99. **Los mecanismos de derechos humanos deben seguir evaluando las obligaciones de los agentes privados de desarrollar y proveer tecnologías de vigilancia.**