Naciones Unidas A/HRC/13/37

Asamblea General

Distr. general
28 de diciembre de 2009
Español
Original: inglés

Consejo de Derechos Humanos
13º 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 la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, Martin Scheinin

Resumen

En el capítulo I del presente informe el Relator Especial destaca las principales actividades que realizó entre el 1º de agosto y el 15 de diciembre de 2009. En el informe principal, que figura en el capítulo II, se ponen de manifiesto diversas preocupaciones del Relator Especial en relación con la protección del derecho a la intimidad en la lucha contra el terrorismo. La importancia del derecho a la intimidad y de la protección de datos se destaca en la sección A.

El artículo 17 del Pacto Internacional de Derechos Civiles y Políticos tiene la flexibilidad suficiente para permitir unas limitaciones necesarias, legítimas y proporcionadas del derecho a la intimidad. En la sección B el Relator Especial sostiene que el artículo 17 se debe interpretar en el sentido de que contiene los elementos necesarios para unas limitaciones admisibles. En este contexto, pide a los Estados que justifiquen la razón de que un objetivo particular constituya una justificación legítima para imponer restricciones al artículo 17, y al Comité de Derechos Humanos que adopte una nueva observación general sobre el artículo 17.

En la sección C el Relator Especial destaca la erosión del derecho a la intimidad en la lucha contra el terrorismo. Esta erosión es consecuencia de la utilización de poderes de vigilancia y nuevas tecnologías sin las salvaguardias legales suficientes. Los Estados han comprometido la protección del derecho a la intimidad al no ampliar las salvaguardias preexistentes en su cooperación con terceros países y actores privados. Estas medidas no solo han conducido a violaciones del derecho a la intimidad sino que también han influido en los derechos a las debidas garantías procesales y en la libertad de circulación —especialmente en las fronteras— y pueden tener un efecto de inhibición en la libertad de asociación y de expresión.

En ausencia de un conjunto riguroso de salvaguardias legales y de una forma de medir la necesidad, proporcionalidad y racionalidad de la injerencia, los Estados no tienen nada que les oriente sobre la forma de minimizar los riesgos que para la intimidad suponen sus nuevas políticas. El Relator Especial identifica en la sección D algunas de las salvaguardias legales que han surgido en la política, la jurisprudencia, el análisis político y las buenas prácticas en todo el mundo.

En la sección final se formulan recomendaciones a los diversos protagonistas (asambleas legislativas nacionales, poder ejecutivo interno y las Naciones Unidas) a fin de mejorar la protección del derecho a la intimidad en la lucha contra el terrorismo.

Índice

		Párrafos	*Página*
I.	Introducción	1–2	4
II.	Actividades del Relator Especial	3–10	4
III.	El derecho a la intimidad	11–57	5
	A. El derecho a la intimidad en su forma reconocida en las constituciones y en los tratados internacionales de derechos humanos	11–13	5
	B. Limitaciones admisibles del derecho a la intimidad	14–19	7
	C. Erosión del derecho a la intimidad como consecuencia de la política antiterrorista	20–47	10
	D. Las mejores prácticas	48–57	19
IV.	Conclusiones y recomendaciones	58–74	22
	A. Conclusiones	58–59	22
	B. Recomendaciones	60–74	23

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 somete el presente informe al Consejo de Derechos Humanos en cumplimiento de la resolución 63/185 de la Asamblea General y de la resolución 10/15 del Consejo de Derechos Humanos. El cuerpo del informe destaca las actividades realizadas por el Relator Especial entre el 1º de agosto y el 15 de diciembre de 2009 y se centra en el tema del derecho a la intimidad como uno de los derechos humanos en el contexto de la lucha contra el terrorismo. Las adiciones contienen un informe de las comunicaciones (A/HRC/13/37/Add.1) y un informe sobre la misión de investigación llevada a cabo en Egipto del 17 al 21 de abril de 2009 (A/HRX/13/37/Add.2).

2. En cuanto a las próximas visitas a países, el Relator Especial espera visitar Túnez antes de presentar este informe. El Relator Especial ha propuesto las fechas de finales de enero y principios de febrero de 2010 y espera una respuesta del Gobierno. El Relator Especial espera también hacer visitas oficiales a Chile y el Perú en 2010. Hay solicitudes de visitas pendientes a Argelia, Filipinas, Malasia, Pakistán y Tailandia.

II. Actividades del Relator Especial

3. Los días 18 y 19 de septiembre de 2009, el Relator Especial reunió un grupo de expertos en el Instituto Universitario Europeo de Florencia para discutir cuestiones temáticas relacionadas con su mandato[1]. La reunión coincidió parcialmente con un acto público sobre la lucha contra el terrorismo y los problemas que plantea al poder judicial, organizado conjuntamente con la Comisión de Venecia y la Subcomisión sobre los problemas relacionados con la delincuencia del Consejo de Europa. La reunión fue cofinanciada por el Instituto de Derechos Humanos de la Universidad Åbo Akademi en el marco de su proyecto de apoyo al mandato del Relator Especial.

4. Los días 29 y 30 de septiembre de 2009 el Relator Especial, junto con otros titulares de mandatos, participó en consultas oficiosas realizadas en Ginebra en relación con un estudio conjunto global sobre la detención secreta (A/HRC/13/42). Se reunió también con representantes de las misiones permanente de Egipto y Túnez en relación con las visitas realizadas o previstas a esos países.

5. Los días 2 y 3 de octubre de 2009, el Relator Especial participó en una Conferencia de Wilton Park sobre el terrorismo, la seguridad y los derechos humanos y las oportunidades de un cambio de política, e intervino como miembro de un grupo de expertos en un debate sobre la función de las organizaciones internacionales en la respuesta al terrorismo y la protección de los derechos humanos.

6. El 4 de octubre de 2009, el Relator Especial pronunció un discurso con ocasión de la inauguración del curso académico en la Facultad de Derecho de la Universidad del País Vasco en Bilbao (España).

7. Del 12 al 14 de octubre de 2009, el Relator Especial participó en dos manifestaciones celebradas en Viena: el taller internacional de coordinadores nacionales para la lucha contra el terrorismo y la reunión del Equipo Especial sobre la Ejecución de la Lucha contra el Terrorismo (CTITF). El taller fue conjuntamente organizado por varios

[1] El Relator Especial expresa su agradecimiento por su ayuda para la preparación del presente informe a los miembros del grupo de expertos, el Dr. Gus Hosein y Mathias Vermeulen, su asistente de investigación, y a los doctorados participantes en el seminario del Instituto Universitario Europeo.

Estados miembros y por la Oficina de las Naciones Unidas contra la Droga y el Delito, en estrecha cooperación con la Oficina del CTITF y la Dirección Ejecutiva del Comité contra el Terrorismo. La reunión permitió un intercambio de opiniones sobre la mejor manera de vincular las actividades nacionales y mundiales de lucha contra el terrorismo fomentando una mayor interrelación entre los coordinadores nacionales de la lucha contra el terrorismo y facilitando su función de enlace entre las actividades nacionales, regionales y mundiales de lucha contra el terrorismo. La reunión del CTITF se centró en la manera de ampliar y fortalecer las relaciones entre los Estados miembros, el sistema de las Naciones Unidas, las organizaciones regionales y de otra índole y la sociedad civil en la ejecución de la Estrategia global de las Naciones Unidas contra el terrorismo[2].

8. El 20 de octubre de 2009, el Relator Especial estuvo representado en un seminario celebrado en Bruselas sobre el fortalecimiento de las sanciones selectivas de las Naciones Unidas a través de procedimientos imparciales y justos, organizado por la Administración pública federal de Bélgica para relaciones exteriores, comercio internacional y cooperación para el desarrollo.

9. Del 26 al 28 de octubre de 2009, el Relator Especial estuvo en Nueva York para presentar a la Tercera Comisión de la Asamblea General su informe[3], que se centraba en las repercusiones en ambos sexos de las medidas de lucha contra el terrorismo. El Relator Especial participó en una reunión oficial con el Comité de Sanciones contra Al-Qaida y los Talibanes del Consejo de Seguridad y se reunió con el director de la Dirección Ejecutiva del Comité contra el Terrorismo. El Relator Especial participó como experto en un evento paralelo sobre la lucha contra el terrorismo y la seguridad nacional organizado por el Centro de Derechos Humanos y Justicia Mundial de la Facultad de Derecho de la Universidad de Nueva York. Se reunió igualmente con diversas organizaciones no gubernamentales (ONG) y dio una conferencia de prensa.

10. El 29 de octubre de 2009, el Relator Especial se reunió con el Vicesecretario de Estado para la democracia, los derechos y el trabajo y otros funcionarios del Departamento de Estado de los Estados Unidos en Washington, D.C., para discutir el marco jurídico actual y futuro con la nueva administración, como complemento de la visita que realizó a los Estados Unidos de América en 2007[4] y otros temas más generales relacionados con la normativa de derechos humanos y el derecho humanitario en el contexto de la lucha contra el terrorismo.

III. El derecho a la intimidad

A. El derecho a la intimidad en su forma reconocida en las constituciones y en los tratados internacionales de derechos humanos

11. La intimidad es un derecho humano fundamental que 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 otras y libre de la intervención del Estado y de la intervención excesiva no solicitada de otros individuos no invitados[5]. El derecho a la intimidad ha evolucionado en dos direcciones diferentes. Los instrumentos universales de

[2] Véase la resolución 60/288 de la Asamblea General.
[3] A/64/211.
[4] Véase A/HRC/6/17/Add.3.
[5] Lord Lester y D. Pannick (eds.), *Human Rigths Law and Practice* (Londres, Butterworth, 2004), párr. 4.82.

derechos humanos se han centrado en la dimensión negativa del derecho a la intimidad, prohibiendo toda injerencia arbitraria en la vida privada, la familia, el domicilio o la correspondencia[6], aunque algunos instrumentos regionales y nacionales han incluido también una dimensión positiva: toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia[7], o el derecho al reconocimiento y respeto de su propia dignidad e integridad personal o buena reputación[8]. Aunque las constituciones no siempre mencionan directamente la intimidad como derecho específico, prácticamente todos los Estados reconocen su valor como materia de importancia constitucional. En algunos países el derecho a la intimidad deriva por extensión del abuso de confianza, el derecho a la libertad, la libertad de expresión o el derecho a las debidas garantías procesales. En otros países el derecho a la intimidad surge como un valor religioso. Por consiguiente, el derecho a la intimidad no es solo un derecho humano fundamental sino también un derecho humano que sirve de apoyo a otros derechos humanos y forma la base de toda sociedad democrática.

12. La capacidad del Estado de desarrollar sistemas de registro aumentó con el desarrollo de la tecnología de la información. El aumento de la capacidad informática permitió formas inimaginables de reunir, almacenar e intercambiar datos personales. Se desarrollaron principios internacionales de protección de datos fundamentales, entre los que figuraba la obligación de: obtener la información personal por procedimientos legales y justos; limitar el ámbito de su uso a los fines inicialmente especificados; asegurar un tratamiento adecuado, pertinente y no excesivo; garantizar su exactitud; mantenerla en seguridad; suprimirla cuando deja de ser necesaria y garantizar al individuo el derecho de acceder a los datos sobre su persona y a solicitar las correcciones oportunas[9]. En su Observación general Nº 16 el Comité de Derechos Humanos proporcionó indicaciones claras en el sentido de que esos principios se encerraban en el derecho a la intimidad[10], pero la protección de datos surge también como un derecho humano o fundamental distinto. Algunos países han recogido la protección de datos incluso como derecho constitucional, subrayando de esta manera su importancia como elemento de la sociedad democrática. Cabe citar aquí como ejemplo de las mejores prácticas el texto detallado del artículo 35 de la Constitución de Portugal de 1976.

13. El derecho a la intimidad no es un derecho absoluto. Cuando un individuo está siendo formalmente investigado o examinado por un organismo de seguridad, la información personal se distribuye entre los organismos de seguridad por motivos

[6] Véase la Declaración Universal de Derechos Humanos (art. 12); el Pacto Internacional de Derechos Civiles y Políticos (art. 17); la Convención Internacional sobre la protección de los derechos de todos los trabajadores migratorios y de sus familiares (art. 14); y la Convención sobre los Derechos del Niño (art. 16).

[7] Véase el Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales (art. 8) y la Declaración de El Cairo sobre Derechos Humanos en el Islam (A/45/421-S/21797, art. 18), 5 de agosto de 1990.

[8] Carta Africana sobre los Derechos Humanos y de los Pueblos (art. 11). Véase también la Declaración de Principios sobre la Libertad de Expresión en África (art. 4.3) y la Declaración Americana de los Derechos y Deberes del Hombre (art. 5).

[9] Véase la Convención para la Protección de las Personas respecto de la computadorización de datos personales (Nº 108), 1981, del Consejo de Europa; las Directrices sobre la protección de la intimidad y de los flujos transfronterizos de datos personales (1980) de la Organización de Cooperación y Desarrollo Económicos; y los Principios rectores para la reglamentación de los ficheros computadorizados de datos personales (resolución 45/95 de la Asamblea General y E/CN.4/1990/72).

[10] Observación general Nº 16 (1988) del Comité de Derechos Humanos sobre el derecho al respeto de la intimidad familiar, el domicilio y la correspondencia y a la protección de la honra y la reputación (art. 17).

derivados de la lucha contra el terrorismo y el derecho a intimidad se ve casi automáticamente afectado. Se trata de situaciones en las que los Estados tienen el poder legítimo de limitar el derecho a la intimidad de acuerdo con las normas internacionales de derechos humanos. No obstante, la lucha contra el terrorismo no es un comodín que legitime automáticamente toda injerencia en el derecho a la intimidad. Cada caso de injerencia debe ser objeto de una evaluación crítica.

B. Limitaciones admisibles del derecho a la intimidad

14. El artículo 17 del Pacto Internacional de Derechos Civiles y Políticos es la disposición convencional de obligado cumplimiento más importante del derecho humano a la intimidad a nivel universal. El Pacto ha sido ratificado por 165 Estados y firmado por otros 6[11]. El artículo 4 del Pacto permite a los Estados partes suspender el cumplimiento de algunas de sus disposiciones, incluido el artículo 17. Estas suspensiones solo podrán hacerse durante un estado de excepción que ponga en peligro la vida de la nación y están sometidas a varias condiciones[12]. A lo largo de los más de treinta años transcurridos desde la entrada en vigor del Pacto en 1976, menos de diez Estados partes han introducido un estado de excepción por motivo de actos o amenazas de terrorismo[13]. Cuatro de ellos han previsto en el mismo contexto suspender la aplicación del artículo 17 del Pacto[14]. Otros ocho han anunciado la suspensión del artículo 17 sin una referencia explícita al terrorismo como causa del estado de excepción[15]. Sin embargo, los anuncios en cuestión han sido más bien genéricos, en vez de especificar, como exige el artículo 4, las disposiciones cuya aplicación se haya suspendido en la medida estrictamente limitada a las exigencias de la situación[16]. En general, no hay un solo Estado que haya tratado de suspender la aplicación del artículo 17 con referencia al terrorismo y que haya podido demostrar el cumplimiento de todos los requisitos del artículo 4. Además, solo un Estado ha anunciado la suspensión del Pacto con referencia a la amenaza actual (relacionada con los sucesos del 11 de septiembre de 2001) del terrorismo internacional[17]. La situación es similar con respecto a las reservas al artículo 17. Aunque el derecho internacional permite generalmente a los Estados introducir reservas a los tratados de derechos humanos, siempre que esas reservas

[11] Al 16 de noviembre de 2009. Los seis países cuya firma no ha sido seguida de la ratificación son China, Cuba, Guinea-Bissau, Nauru, Panamá y San Marino.

[12] En cuanto a la postura del órgano competente de supervisión de tratados sobre el ámbito y efecto de las suspensiones, véase la Observación general Nº 29 (2001) del Comité de Derechos Humanos.

[13] Azerbaiyán, Chile, Colombia, El Salvador, Federación de Rusia, Israel, Nepal, Perú y Reino Unido de Gran Bretaña e Irlanda del Norte.

[14] Colombia, El Salvador, Federación de Rusia y Nepal.

[15] Argelia, Armenia, Ecuador, Nicaragua, Panamá, República Bolivariana de Venezuela, Serbia y Montenegro y Sri Lanka. En algunos de estos casos puede haber habido un nexo factual con el terrorismo, aunque no se mencionaba en el anuncio de la introducción del estado de excepción.

[16] Por ejemplo, al tratar de suspender la aplicación del Pacto Internacional de Derechos Civiles y Políticos, muchos Estados latinoamericanos han notificado claramente que se "suspenderá la aplicación" de algunas disposiciones del Pacto específicamente citadas. Ello no se ajusta a las exigencias del artículo 4, como se explica en la Observación general Nº 29.

[17] El Reino Unido, el 18 de diciembre de 2001. Las suspensiones no incluían el artículo 17 y fueron suprimidas el 15 de marzo de 2005.

no sean incompatibles con el objeto y el fin del tratado[18], solamente un Estado parte ha presentado una reserva al artículo 17[19].

15. Parece por consiguiente que los Estados han recurrido solo en contadas ocasiones a los mecanismos reconocidos y disponibles en el derecho internacional en general y en el Pacto en particular para introducir excepciones unilaterales al derecho a la intimidad. Incluso en los casos en que se ha anunciado la suspensión de la aplicación del artículo 17, las denuncias han sido genéricas, en vez de hacer referencia a medidas prácticas y a formas específicas de suspensión. Para el Relator Especial esa práctica de los Estados demuestra que en general los Estados parecen satisfechos de que el marco del artículo 17 sea lo bastante flexible para permitir la introducción de las restricciones necesarias, legítimas y proporcionadas del derecho a la intimidad por medio de limitaciones admisibles, incluso en los casos de respuesta al terrorismo. El Relator Especial apoya esta opinión. La redacción del artículo 17 ofrece a los Estados partes la posibilidad de introducir restricciones o limitaciones de los derechos reconocidos en la disposición, incluso el derecho a la intimidad. Por consiguiente, esas restricciones y limitaciones estarán sometidas a las funciones de supervisión del Comité de Derechos Humanos como órgano convencional encargado de la tarea de interpretar las disposiciones del Pacto y dirigir la conducta de los Estados partes en lo que respecta a sus obligaciones convencionales. Los mecanismos principales para el ejercicio de esas funciones son el procedimiento de presentación obligatoria de informes previsto en el artículo 40 del Pacto y para los 113 Estados que han ratificado el primer Protocolo Facultativo del mismo, el procedimiento de comunicaciones individuales.

16. El artículo 17 del Pacto prohíbe las injerencias "arbitrarias o ilegales" en la vida privada, la familia, el domicilio o la correspondencia, así como los "ataques ilegales" a la honra y reputación de una persona. Cabe comparar este texto con la formulación de otras disposiciones como el párrafo 3 del artículo 12, el párrafo 3 del artículo 18, el párrafo 3 del artículo 19, el artículo 21 y el párrafo 2 del artículo 22, que describen los elementos de prueba de la admisibilidad de las limitaciones. En su forma más precisa esta prueba se describe en el artículo 21 y en el párrafo 3 del artículo 22 y consta de los tres elementos siguientes: a) las restricciones deben estar expresamente fijadas por la ley; b) deben ser necesarias en una sociedad democrática; y c) deben ser en interés de uno de los objetivos legítimos enumerados en cada una de las disposiciones que contiene una cláusula limitativa.

17. El Relator Especial considera que pese a las diferencias de redacción, el artículo 17 del Pacto debe ser interpretado en el sentido de que contiene los elementos mencionados de prueba de la admisibilidad de la limitación. Las restricciones no prescritas por la ley son "ilegales" en el sentido del artículo 17, y las restricciones que distan de ser necesarias o no responden a un objetivo legítimo constituyen una injerencia "arbitraria" en los derechos previstos por el artículo 17. Por consiguiente, las limitaciones del derecho a la intimidad o de otras dimensiones del artículo 17 están sometidas a una prueba de admisibilidad, como establece el Comité de Derechos Humanos en su Observación general Nº 27 (1999). Esa observación general hace referencia a la libertad de circulación (art. 12) que es una de las disposiciones que contiene una cláusula limitativa. Al mismo tiempo, codifica la postura del Comité de Derechos Humanos en la materia de las limitaciones admisibles a los derechos previstos por el Pacto. La prueba de la admisibilidad de las limitaciones, en los

[18] En cuanto a la postura del órgano competente de supervisión de tratados con respecto a las reservas al Pacto Internacional de Derechos Civiles y Políticos y sus Protocolos Facultativos, véase la Observación general Nº 24 (2004) del Comité de Derechos Humanos.

[19] Liechtenstein mantiene una reserva sobre el ámbito del derecho al respeto de la vida familiar en relación con los extranjeros.

términos expresados en la observación general, incluye, entre otros, los elementos siguientes:

a) Las restricciones deben estar previstas por la ley (párrs. 11 y 12);

b) Las restricciones no deben comprometer la esencia del derecho (párr. 13);

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

d) El poder discrecional de aplicación de las restricciones no debe ser ilimitado (párr. 13);

e) Para que una restricción sea admisible no basta con que se utilice para conseguir fines legítimos; debe ser necesaria para lograrlos (párr. 14);

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

g) Las restricciones deben ser compatibles con los demás derechos consagrados en el Pacto (párr. 18)[20].

18. El Relator Especial opina que estas consideraciones son también aplicables al artículo 17 del Pacto en tanto que interpretaciones de las nociones de "ilegalidad" y "arbitrariedad". No obstante, la diferencia realmente importante de redacción entre el artículo 17 y las disposiciones del Pacto que introducen explícitamente una prueba de admisibilidad de las limitaciones reside en la ausencia de una lista exhaustiva de objetivos legítimos en el artículo 17. El Relator Especial pide aquí a los Estados que justifiquen la razón de que un objetivo particular constituya una justificación legítima de la imposición de restricciones al artículo 17, y al Comité de Derechos Humanos que continúe supervisando las medidas adoptadas por los Estados partes, en particular a través del examen de los informes periódicos y de las comunicaciones individuales.

19. A juicio del Relator Especial, el Comité de Derechos Humanos debería redactar y aprobar una nueva observación general sobre el artículo 17, en sustitución de la actual Observación general Nº 16 (1988). La observación general existente es muy breve y no refleja el grueso de la práctica del Comité durante los más de 20 años transcurridos desde su aprobación. Sin embargo, muchos de los elementos de una cláusula limitativa adecuada, presentados en los párrafos anteriores a la luz de la posterior Observación general Nº 27, existían ya en 1988[21]. En su jurisprudencia posterior en el marco del Protocolo Facultativo, el Comité ha insistido en que la injerencia en los derechos previstos en el artículo 17 debe satisfacer simultáneamente varias condiciones: debe estar prevista por la ley, debe estar de acuerdo con las disposiciones, fines y objetivos del Pacto y debe ser razonable en las circunstancias particulares del caso[22]. Además, en su determinación de las violaciones del artículo 17 el Comité ha aplicado los requisitos del objetivo legítimo, la necesidad y la proporcionalidad[23].

[20] Véase la Observación general Nº 27 (1999) del Comité de Derechos Humanos.

[21] Véase la Observación general Nº 16 (1988) del Comité de Derechos Humanos. Véanse, en particular, los párrafos 3 y 4 que se extienden sobre las nociones de injerencia arbitraria o ilegal en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos.

[22] Véase la comunicación Nº 903/1999, 2004, *Van Hulst c. los Países Bajos*.

[23] Véase *Madafferi c. Australia*, comunicación Nº 1011/2001, 2004, *y M. G. c. Alemania*, comunicación Nº 1482/2006, 2008.

C. Erosión del derecho a la intimidad como consecuencia de la política antiterrorista

20. Al examinar la política antiterrorista actual, los Estados suelen sostener que existen dos nuevas dinámicas que es preciso analizar paralelamente a la protección de la intimidad. En primer lugar, los Estados pretenden que su capacidad de prevenir e investigar actos terroristas va estrechamente unida al aumento de los poderes de vigilancia. En consecuencia, la mayoría de las leyes antiterroristas promulgadas desde los acontecimientos del 11 de septiembre de 2001 se han centrado en ampliar el poder de vigilancia de los gobiernos. En segundo lugar, los Estados sostienen que al ser el terrorismo una actividad mundial, la búsqueda de terroristas debe realizarse también más allá de las fronteras nacionales, con ayuda de terceras partes que dispongan de información abundante sobre ciertos individuos, que se pueda utilizar como recurso para identificar y vigilar a terroristas sospechosos. Los Estados que anteriormente carecían de salvaguardias constitucionales o legislativas han podido transformar radicalmente sus poderes de vigilancia con escasas limitaciones. En los países que disponen de salvaguardias constitucionales y legales, los gobiernos han puesto en peligro la protección del derecho a la intimidad al no extender esas salvaguardias a su cooperación con terceros países y con el sector privado o al situar los sistemas de vigilancia fuera de la jurisdicción de sus constituciones.

1. Aumento de las medidas de vigilancia

21. Las operaciones de vigilancia pueden ser generales o específicas. A nivel específico, los sistemas jurídicos pueden autorizar y supervisar: formas encubiertas y abiertas de vigilancia para identificar conductas ilegales; la acumulación de información sobre individuos específicos para identificar el incumplimiento de la ley y la vigilancia específica de individuos para instruir un procedimiento judicial. El Relator Especial ha señalado ya que los Estados pueden recurrir a medidas de vigilancia específicas siempre que se trate de injerencias en casos concretos, sobre la base de una orden judicial por una causa probable o por motivos fundados. Tiene que haber alguna base de hecho, relacionada con el comportamiento de una persona, que justifique la sospecha que pueda estar preparando un atentado terrorista[24]. A nivel general, ha habido un aumento en la vigilancia de las comunicaciones a través de la interceptación de comunicaciones por las fuerzas de seguridad y los servicios de inteligencia. Se advierte una convergencia notable en las políticas aplicadas para aumentar los poderes de vigilancia en respuesta a las amenazas terroristas. La mayoría de esas políticas se basan en tecnologías nuevas o existentes, como los errores de *software* y las tecnologías de rastreo que pueden acceder a la posición geográfica de los teléfonos móviles, las tecnologías que dan cuenta a los gobiernos del contenido de conversaciones privadas de usuarios de voz en el protocolo de Internet[25] o que instalan programas espías en los ordenadores de los sospechosos a fin de hacer posible el acceso remoto a los mismos[26]. En algunos países los servicios de seguridad han llegado incluso a proponer la supresión de las tecnologías de comunicación que son más difíciles de

[24] A/ARC/10/3, párr. 30.

[25] D. O'Brien, "Chinese Skype client hands confidential communications to eavesdroppers", Electronic Fontier Foundation, 2 de octubre de 2008.

[26] Véase el artículo que aparece en la dirección siguiente: http://www.bundestag.de/dokumente/textarchiv/2008/22719940_kw46_bka/index.html.

interceptar, como los teléfonos inteligentes[27]. Preocupa asimismo al Relator Especial el rastreo de las comunicaciones transfronterizas sin autorización judicial[28].

22. En nombre de la lucha contra el terrorismo, los Estados han aumentado las iniciativas para identificar, examinar y controlar al público en general mediante el uso de una multitud de técnicas que podrían violar el derecho del individuo a la intimidad. Cuando se vigilan lugares y grupos nutridos de personas, la vigilancia suele estar sometida a un régimen menos estricto de autorización y supervisión. Las normas de derechos humanos se han puesto a prueba, violentado e infringido con el uso de registros, la compilación de listas y bases de datos, la creciente vigilancia de las comunicaciones financieras y los datos de viaje, el uso de perfiles para identificar a posibles sospechosos y la acumulación de bases de datos cada vez mayores para calcular la probabilidad de actividades sospechosas e identificar a los individuos a los que se consideran merecedores de una investigación más minuciosa. Se aplican también tecnologías más avanzadas como la reunión de datos biométricos o la utilización de escáneres corporales que permiten ver a través de la ropa[29]. Algunas intrusiones en la vida de las personas pueden llegar a ser permanentes ya que los detalles físicos y biográficos de las personas se suelen centralizar en bases de datos.

a) Poderes de detención y registro

23. Los Estados han ampliado sus poderes de detención, interrogatorio, registro e identificación de individuos y han reducido los controles establecidos para evitar el abuso de esos poderes. Tales poderes han dado lugar al nacimiento de preocupaciones sobre el perfil y la discriminación racial en Europa[30] y en la Federación de Rusia[31] y a la preocupación de que estos poderes antagonicen la relación entre los ciudadanos y el Estado. Igualmente, la exigencia de proporcionalidad en la prueba de admisibilidad de las limitaciones al derecho a la intimidad plantea la cuestión de si un poder general de detención y registro en zonas de seguridad designadas, como sucede en la Federación de Rusia[32] o el Reino Unido[33], es realmente necesario en una sociedad democrática.

b) El uso de datos biométricos y los peligros de los sistemas centralizados de identificación

24. Un componente fundamental de las políticas de identificación es la utilización de técnicas biométricas como el reconocimiento facial, las huellas dactilares y el examen del iris. Aunque en algunas circunstancias estas técnicas puedan ser un instrumento legítimo para la identificación de terroristas sospechosos, preocupan especialmente al Relator Especial los casos en que los datos biométricos no se almacenan en un documento de identidad sino en una base central de datos, aumentando de esta manera los riesgos de seguridad de la información y haciendo vulnerables a los individuos. Con el aumento de la obtención de información biométrica, las tasas de error pueden crecer de manera

[27] S. Das Gupta y L. D'Monte, "BlackBerry security issue makes e-com insecure", *Business Standard*, 12 de marzo de 2008.

[28] Véase por ejemplo la Ley del Gobierno sueco sobre las operaciones ajustadas de inteligencia de defensa, aprobada en junio de 2008, pág. 83.

[29] Véase la resolución del Parlamento Europeo del 23 de octubre de 2008 sobre el impacto de las medidas de seguridad de la aviación y los escáneres corporales en los derechos humanos, la privacidad, la dignidad personal y la protección de datos.

[30] Open Society Justice Initiative, *Ethnic Profiling by Police in Europe*, junio de 2005.

[31] Open Society Justice Initiative and JURIX, *Ethnic Profiling in the Moscow Metro*, junio de 2006.

[32] Ley Federal Nº 35 de 2006 sobre la lucha contra el terrorismo.

[33] Véase, por ejemplo, Tribunal de Apelaciones del Reino Unido, *R. c. Commissioner of Police for the Metropolis and another*, 2006.

significativa[34]. Ello puede traducirse en la criminalización de personas o en la exclusión social. Entretanto, a diferencia de otros datos identificadores, los datos biométricos no se pueden revocar: una vez copiados y utilizados fraudulentamente por un tercero de mala fe, no es posible atribuir al individuo una nueva firma biométrica[35]. En este contexto, conviene advertir que, contrariamente a su objetividad científica, las pruebas de ADN pueden ser también falsificadas[36].

25. La reunión centralizada de datos biométricos crea el riesgo de causar errores judiciales, como puede verse por el ejemplo siguiente. Todos los atentados con bomba que se produjeron en Madrid el 11 de marzo de 2004, la policía española encontró una huella dactilar en una bomba que no había hecho explosión. Expertos en huellas dactilares de la Oficina Federal de Investigación (FBI) de los Estados Unidos declararon que la huella dactilar de un abogado coincidía con la muestra obtenida en el lugar del atentado. La huella dactilar de la persona se encontraba almacenada en el sistema nacional porque esa persona había sido soldado de los Estados Unidos. El individuo fue detenido y mantenido en régimen de aislamiento durante dos semanas aunque la huella dactilar no era la suya. Los inspectores no procedieron a una nueva comparación, con lo que la situación se complicó para el detenido cuando se descubrió que había sido el abogado defensor de un terrorista convicto, se había casado con una inmigrante egipcia e incluso se había convertido al islam[37].

c) La distribución de listas secretas de control

26. Otra técnica disponible es la supervisión de listas de control. El tipo más común de estas listas es la lista de personas sometidas a la prohibición de volar. Esas listas se distribuyen a las líneas áreas y a los agentes de seguridad con la instrucción de detener e interrogar a los pasajeros que lleven cierto nombre. Poco se sabe de la medida en que se usan estas listas pero cuando esos sistemas salen a la luz pública, se descubren errores y surgen preocupaciones en cuanto a la intimidad de las personas, particularmente en los Estados Unidos[38] y el Canadá[39]. Subsisten los problemas de integridad de los datos, pues las listas son objeto de comprobaciones continuas para descubrir posibles errores y los procesos de identificación se deben realizar con el mayor cuidado. Las listas se suelen mantener secretas pues podrían servir de aviso a los terroristas sospechosos, pero al mismo tiempo este secretismo plantea problemas al mantener bajo vigilancia constante sin una supervisión independiente efectiva a individuos que desconocen que figuran en algún tipo de lista. Esa vigilancia secreta podría constituir una violación del derecho a la intimidad previsto en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos.

27. Cuando se hacen públicas las listas de terroristas, surge una nueva forma de aplicar el artículo 17 del Pacto. El Comité de Derechos Humanos ha determinado que la inclusión injustificada de una persona en la Lista Consolidada del Comité 1267 de las Naciones

[34] Véase por ejemplo, M. Cherry y E. Imwinkelried, "A cautionary note about fingerprint analysis and reliance on digital techonology", *Judicature*, vol. 89, Nº 6 (2006).

[35] Véase E. Kosta y otros, "An analysis of security and privacy issues relating to RFID enabled ePassports", International Federation for Information Processing, Nº 232 (2007), págs. 467 a 472.

[36] Véase por ejemplo, D. Frumkin y otros, "Authentification of forensic DNA samples" *Forensic Science International: Genetics* (17 de julio de 2009).

[37] Véase Departamento de Justicia de los Estados Unidos, Oficina del Inspector General, *A Review of the FBI's Handling of the Brandon Mayfield Case*, enero de 2006.

[38] Véase Departamento de Justicia de los Estados Unidos, *Audit of the FBI Terrorist Watchlist Nomination Practices*, mayo de 2009.

[39] Véase Office of the Privacy Commissioner Canada, *Audit of the Passenger Protect Program of Transport Canada*, noviembre de 2009.

Unidas constituía una violación del artículo 17. Estimó que la divulgación de información personal constituía un ataque a la honra y reputación de las personas incluidas en la lista dada la asociación negativa que podría hacerse entre los nombres y el título de la lista de sanciones[40].

28. Las listas públicas y secretas de control suelen incumplir también principios fundamentales de la protección de datos. La información obtenida con una finalidad se vuelve a utilizar con finalidades secundarias y se intercambia a veces con otras instituciones, sin el conocimiento o consentimiento de las personas afectadas. Se utiliza información errónea para adoptar decisiones sobre personas que se traducen en limitaciones para viajar. Puede suceder que a esas personas se les deniegue un visado, se les devuelva en la frontera o se les impida subir a bordo de un avión sin pruebas de que hayan cometido alguna infracción.

d) Puntos de control y fronteras

29. Con la aplicación de nuevas tecnologías y en respuesta a temores crecientes de la comisión de atentados terroristas, los Estados aumentan la vigilancia, reglamentación, intervención y control de la circulación de personas en las fronteras. En la actualidad y con la aplicación de tecnologías más adelantadas y de acuerdos de intercambio de datos, los Estados están creando perfiles amplios de viajeros extranjeros a fin de identificar a terroristas y delincuentes antes de que lleguen a la frontera, estudiando para ello las listas de pasajeros y los registros de reserva de pasaje de las empresas de transporte. Los Estados analizan esta información para identificar perfiles que correspondan a terroristas o delincuentes. En la frontera los individuos se ven sometidos a nuevos métodos de obtención de información, potencialmente invasivos.

30. Muchos Estados piden en la actualidad a las líneas aéreas que faciliten la lista de pasajeros antes del despegue. Los Estados tratan también de obtener acceso a los registros de nombres de pasajeros, que incluyen información sobre la identidad (nombre, número de teléfono) información sobre la transacción (fecha de la reserva, agencia de viajes, itinerario), información sobre el vuelo y el asiento, datos financieros (número de la tarjeta de crédito, dirección de facturación), elección del menú e información sobre el lugar de residencia, datos médicos, información sobre viajes anteriores e información de viajero frecuente. Esta información se utiliza para la elaboración del perfil y la evaluación del riesgo de los pasajeros, generalmente tras consultar las diversas listas de control de terroristas y las bases de datos de las fuerzas de seguridad. Como resultado, las líneas aéreas pueden negarse a conceder la tarjeta de embarque a un individuo solamente sobre la base de los resultados de la consulta de una base de datos situada en el país de destino sin ninguna garantía procesal.

31. La creciente vigilancia de los inmigrantes y de los viajeros con distintas finalidades da lugar a diversas preocupaciones en relación con la intimidad. Los Estados obtienen información sobre los viajeros de terceras partes que están obligadas a facilitarla si no quieren verse privadas de los derechos de aterrizaje o pagar fuertes multas, aun en el caso de que las garantías de intimidad no satisfagan las prescripciones del derecho interno en la materia. Además, es posible que no se conceda a los extranjeros igualdad de acceso a los recursos judiciales en esos países y los derechos en la frontera suelen estar notablemente restringidos. La política del Gobierno de los Estados Unidos sobre el acceso a los ordenadores personales de los viajeros es un ejemplo útil. Pese a la necesidad de satisfacer las exigencias constitucionales del respeto de las debidas garantías al registrar un ordenador

[40] Véase la comunicación Nº 1472/2006 del Comité de Derechos Humanos, párrs. 10.12 y 10.13.

personal en los Estados Unidos, el Departamento de Seguridad Interior ha aprobado el acceso a los ordenadores de los viajeros sin autorización judicial[41].

32. Por último, los Estados están estableciendo nuevas exigencias en materia de información. Los Estados pueden denegar la entrada a personas que se nieguen a facilitar información e insistir en su petición de información sin dar las garantías de que quien solicita esa información es una autoridad legítima. Además, la información obtenida con una finalidad se utiliza con fines distintos; por ejemplo, se ha propuesto la extensión del Sistema automatizado de identificación de huellas dactilares (EURODAC) de la Unión Europea, empleado actualmente para tramitar las peticiones de los solicitantes de asilo y de los inmigrantes ilegales tras su identificación por sus huellas dactilares, a la prevención, detección e investigación de actos de terrorismo y otros delitos graves. El Supervisor de la Protección de Datos de la Unión Europea ha expresado sus dudas en cuanto a si estas propuestas son legítimas según el derecho a la intimidad[42].

2. La vigilancia y su efecto en otros derechos

33. Los regímenes de vigilancia adoptados como medidas antiterroristas han ejercido un profundo efecto de inhibición en otros derechos humanos fundamentales. Además de constituir en sí un derecho, la intimidad es la base de otros derechos cuyo disfrute efectivo sería imposible sin ella. La intimidad es necesaria para crear zonas que permitan a las personas y grupos de personas pensar y desarrollar ideas y relaciones. Otros derechos como la libertad de expresión, asociación y circulación necesitan la intimidad para su disfrute efectivo. La vigilancia se ha traducido también en errores judiciales, en inobservancia de las garantías procesales y en detenciones ilegales.

34. En muchas naciones de todo el mundo se vigila a los ciudadanos, los lugares que visitan y las personas con las que se relacionan. En Alemania se determinó que en 2006 el Servicio de Inteligencia Federal había espiado ilegalmente a periodistas vigilando sus comunicaciones y situando espías en las salas de prensa[43]. En Colombia se demostró en 2009 que el Departamento Administrativo de Seguridad venía sometiendo a vigilancia ilegal desde hacía siete años a periodistas, trabajadores de derechos humanos, funcionarios públicos y jueces y sus familias[44]. En numerosos países de todo el mundo los usuarios de Internet deben identificarse y sus sesiones quedan grabadas para su futuro uso por las autoridades. Por ejemplo, en 2007 se exigió a los proveedores del servicio de Internet de Bangladesh que facilitaran a las autoridades la identidad y las contraseñas de sus usuarios. Algunos de ellos recibieron después la visita de las autoridades, que analizaron sus ordenadores y listas de contactos[45]. En los Estados Unidos la dependencia antiterrorista del FBI supervisó los movimientos de activistas pacíficos durante las convenciones políticas de 2004[46]. Estas medidas de vigilancia han ejercido un efecto disuasorio sobre los usuarios, que temen entrar en Internet, expresar sus opiniones o establecer comunicaciones con otras

[41] Véase Departamento de Seguridad Interior, *Privacy impact assessment for the border searches of electronic devices*, 25 de agosto de 2009.

[42] Véase la declaración del Supervisor de Protección de Datos de la Unión Europea sobre el acceso de las fuerzas de seguridad a EURODAC, 8 de octubre de 2009.

[43] Deutsche Welle World, "Germany stops journalist spying in wake of scandal", 15 de mayo de 2006.

[44] Véase *Semana*, 21 de febrero de 2009.

[45] Véase *E-Bangldeshi*, "Crackdown on internet users in Bangladesh", 3 de octubre de 2007 (traduciendo informes de la BBC).

[46] Veáse American Civil Liberties Union, "ACLU uncovers FBI Surveillance of main peace activists", 25 de octubre de 2006.

personas por temor a sanciones[47]. Esto se aplica especialmente a los individuos disidentes, a los que se puede disuadir de ejercer su derecho democrático de protesta contra la política del Gobierno.

35. Además de los poderes de vigilancia, muchas leyes antiterroristas exigen al individuo que revele proactivamente información y conceden amplios poderes a los funcionarios para que soliciten la información necesaria para las investigaciones. En este contexto el Relator Especial ha expresado ya su preocupación por el uso de las cartas de seguridad nacional en los Estados Unidos[48]. Algunos países han ampliado este poder para exigir la revelación de información inicialmente obtenida con fines periodísticos. En Uganda la Ley antiterrorista de 2002 permite las escuchas telefónicas y el registro de los medios de comunicación cuando existan motivos razonables especiales para creer que la información tiene un valor sustancial en las investigaciones antiterroristas[49]. El Relator Especial subraya que el interés legítimo por la revelación de material confidencial de los periodistas solo supera al interés público por la no revelación cuando se demuestra la existencia de una necesidad manifiesta de esa revelación, cuando las circunstancias son de una naturaleza grave y vital y cuando la necesidad de la revelación responde a una necesidad social urgente[50].

36. Los derechos a la libertad de asociación y reunión se ven también amenazados por la vigilancia. Estas libertades suelen requerir reuniones y comunicaciones privadas que permitan a las personas organizarse frente a los gobiernos u otros actores poderosos. El aumento de la vigilancia ha llevado en algunas ocasiones a una "desvirtuación de funciones", cuando la policía o los organismos de inteligencia han calificado de terroristas a otros grupos a fin de permitir la utilización de los poderes de vigilancia concedidos únicamente para la lucha contra el terrorismo. En los Estados Unidos, manifestantes en favor del medio ambiente y de otros conceptos pacíficos fueron incluidos en listas de control de terroristas por la policía del Estado de Maryland antes de las convenciones políticas de Nueva York y de Denver[51]. En el Reino Unido se suelen utilizar cámaras de vigilancia en las manifestaciones de protesta y sus imágenes se almacenan en una base de datos[52]. Una reciente encuesta realizada en el Reino Unido permitió averiguar que una tercera parte de la población se inclina a no participar en manifestaciones de protesta por temor a injerencias en su intimidad[53].

37. La libertad de circulación puede también verse sustancialmente afectada por la vigilancia. La creación de listas secretas de control, la reunión y el intercambio de cantidades excesivas de datos y la imposición de escáneres o exámenes biométricos intrusivos crean nuevas barreras a la movilidad. Como queda dicho en secciones precedentes, ha habido un aumento sustancial en la reunión de información sobre personas que realizan viajes nacionales e internacionales. La información se intercambia de manera

[47] Véase D. S. Sidhu, "The chilling effect of government surveillance programs on the use of the Internet by Muslim-Americans", *University of Maryland Law Journal of Race, Religion, Gender and Class*, vol. 7 (2007), pág. 375.

[48] A/HRC/6/17/Add.3, párr. 51.

[49] Ley antiterrorista, tercera lista, párr. 8.

[50] Véase también la recomendación Nº R (2000) 7, del Comité de Ministros del Consejo de Europa a los Estados miembros sobre el derecho de los periodistas a no revelar sus fuentes de información y Ontario Superior Court of Justice, *O'Neill v. Canada (Attorney General)*, 2006, párr. 163.

[51] Véase L. Rein y J. White, "More groups than thought monitored in police spying", *The Washington Post*, 4 de enero de 2009.

[52] Véase P. L. Lewis y M. Vallée, "Revealed: police databank on thousands of pratesters", *The Guardian*, 6 de marzo de 2009.

[53] Véase A. Jha y J. Randerson, "Poll shows public disquiet about policing at environmental protests", *The Guardian*, 25 de agosto de 2009.

rutinaria y se utiliza para preparar listas de control que han supuesto nuevas barreras a los viajes. Cuando los perfiles y las listas de control se elaboran utilizando información procedente de distintas fuentes y de fiabilidad diversa, el individuo desconoce la fuente de la información, no puede discutir su veracidad ni impugnar las conclusiones formuladas por las autoridades extranjeras. Un mosaico de datos procedentes de bases múltiples puede dar lugar a que los algoritmos de búsqueda identifiquen a personas inocentes como amenazas[54]. Cuando se prohíbe a una persona abandonar el país, el Estado debe exponer las razones por las que se limita la libertad de circulación. De no ser así es probable que el Estado viole el artículo 12 del Pacto Internacional de Derechos Civiles y Políticos[55].

38. Uno de los efectos más graves de las medidas de vigilancia reside en que pueden conducir a errores judiciales y violar las garantías procesales. El problema de conseguir acceso al examen judicial consiste en que algunos regímenes jurídicos pueden impedir el acceso a los tribunales a menos que la persona pueda demostrar que se ha producido la injerencia, algo imposible debido al carácter secreto de los programas de vigilancia. El individuo no puede probar ni demostrar que está realmente sometido a vigilancia. Como consecuencia, el individuo no puede buscar amparo en los tribunales. En casos concretos los tribunales han declarado que los individuos carecían de legitimación al no poder demostrar que se encontraban bajo vigilancia y las lesiones que sufrían se consideraron especulativas[56]. En otros casos, cuando se puede demostrar la injerencia, los Estados han invocado algunas veces el "secreto de Estado" para evitar el examen de proyectos de vigilancia ilegal[57]. El Relator Especial elogia el criterio del Tribunal Europeo de Derechos Humanos, según el cual el individuo no necesita demostrar que esas medidas se le han aplicado necesariamente[58].

3. Extensión de las fronteras jurídicas

39. Los tratados de asistencia jurídica mutua tienen por objeto permitir a los países cooperar en las investigaciones e intercambiar información en casos específicos[59]. También se han concertado acuerdos que permiten el intercambio de información sobre personas que realizan actividades, por ejemplo todos los pasajeros que viajan a otro país o todos los individuos que realizan transacciones financieras interbancarias. Más opacos son los acuerdos entre organismos de inteligencia para intercambiar bases de datos e información. Esas bases de datos suelen disfrutar de amplias excepciones en la aplicación del sistema jurídico interno. Incluso cuando se aplica la legislación interna, los datos pueden referirse a extranjeros no autorizados a invocar ningún derecho ante los tribunales nacionales. Es posible que los individuos desconozcan que están bajo vigilancia —por ejemplo que figuran en una lista de terroristas sospechosos— porque las listas de los organismos de inteligencia no son públicas, y ello hace que no puedan pedir su revisión. Cuando la lista se distribuye a escala internacional, el individuo desconoce las razones de su primera inclusión

[54] Véase Consejo de Investigación Nacional de los Estados Unidos, *Protecting Individual Privacy in the Struggle Against Terrorist: A Framework for Assessment, Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals*, octubre de 2008.

[55] Véase, por analogía, Comité de Derechos Humanos, *B. Zoolfia c. Uzbekistán*, comunicación Nº 1585/2007, 2009, párr. 8.3.

[56] La conclusión más reciente a este respecto se encuentra en *Amnesty International et al. v. John McConnell et al.*, United States District Court for the Southern District of New York, 20 de agosto de 2009.

[57] Véase United States District Court for the Northern District of California, *Al-Haramain Islamic Foundation et al. v. Bush et al.*, 1º de mayo de 2009.

[58] Véase Tribunal Europeo de Derechos Humanos, *Klass v. Germany*, 6 de septiembre de 1978, párr. 38.

[59] Véase G. Hosein, *International Co-operation as a Promise and a Threat, in Cybercrime and Jurisdiction: A Global Suervey* (T. M. C. Asser Press), 2006.

en ella y no puede conseguir su eliminación de las múltiples listas que aparecieron a partir de entonces.

40. Los Estados han aumentado no solamente su cooperación mutua en la lucha contra el terrorismo sino también su colaboración con terceras partes privadas que disponen de información personal sobre individuos a fin de identificar y vigilar a los terroristas sospechosos. Algunos gobiernos han puesto entonces en peligro la protección del derecho a la intimidad al no extender las garantías nacionales de intimidad a su cooperación con terceros países y con actores privados.

41. Ciertas terceras partes, como los bancos, las compañías telefónicas o incluso los cibercafés poseen en la actualidad amplia información personal sobre muchos individuos. Por consiguiente, el acceso a esta información proporciona detalles significativos sobre la vida privada de esos individuos. Al mismo tiempo, los organismos estatales pueden acceder a esta información con menos restricciones que si la información obrara en poder de los propios individuos en su domicilio o incluso en poder de otros organismos del gobierno. En los Estados Unidos, por ejemplo, el Tribunal Supremo ha determinado que como los datos facilitados a terceras partes tales como los bancos o las compañías telefónicas se intercambian "libremente" entre esas partes, los individuos no pueden razonablemente esperar la intimidad[60]. Cuando no existe la protección constitucional que requiere una base jurídica para la injerencia en la vida privada de los individuos, corresponde a la organización privada decidir la forma de responder a la petición del organismo gubernamental. Por lo general el sector privado prefiere que el Gobierno establezca una base legal que obligue a las organizaciones a facilitar la información personal que se les pida, pues ello les libera de la obligación de examinar la naturaleza del caso.

42. Se pide cada vez más a terceros que reúnan más información de la necesaria y que la conserven durante períodos más dilatados de tiempo. Así, el Reino Unido ha propuesto que las compañías de telecomunicaciones vigilen y conserven información sobre las actividades de los individuos en línea, incluidas las actividades a través de las redes sociales, información que tales compañías no tienen interés justificado en reunir[61]. Análogamente, la directiva sobre la conservación de datos de la Unión Europea[62] ha dado lugar a considerables críticas. Cuando en 2008 el Tribunal Constitucional Federal de Alemania suspendió temporalmente la ley alemana por la que se desarrollaba esa directiva, señaló que la conservación de datos sensibles, amplios y sin motivo sobre prácticamente todo el mundo con fines gubernamentales que en el momento del almacenamiento de los datos no se pueden prever detalladamente, puede tener un efecto intimidador considerable[63]. También en Alemania las investigaciones demostraron que las políticas de conservación de datos tenían un efecto disuasorio: el 52% de las personas entrevistadas dijo que probablemente no utilizaría las telecomunicaciones para entrar en contacto con asesores de drogadictos, psicoterapeutas o asesores matrimoniales debido a las leyes de conservación de datos[64].

---

[60] Véase Tribunal Supremo de los Estados Unidos, *Smith v. Maryland*, 1979, en el caso de datos de comunicaciones, y *United States v. Miller*, 1976, en el caso de información financiera.

[61] Véase British All Party Parliamentary Group on Privacy, *Briefing Paper: Inquiry into communications data surveillance proposals and the Interception Modernisation Programme*, junio de 2009.

[62] Directiva 2006/24/CE del Parlamento Europeo y del Consejo de 15 de marzo de 2006 sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la directiva 2002/58/CE, *Diario Oficial*, L 105 (2006), págs. 54 a 63.

[63] Decisión del Tribunal Constitucional Nº 256/08, 11 de marzo de 2008.

[64] Instituto Alemán Forsa, *Meinungen der Bunderburger zur Vorratsdatanspeicherung*, 28 de mayo de

43. En este contexto, preocupa al Relator Especial que en muchos países se hayan aprobado las leyes de conservación de datos sin haberse establecido ninguna garantía legal en cuanto al acceso a esa información o sin haber considerado el hecho de que los nuevos avances tecnológicos están enturbiando la diferencia entre el contenido y los datos de las comunicaciones. Aunque las disposiciones constitucionales tienden a exigir garantías en cuanto al acceso al contenido de las comunicaciones, la protección de los registros de transacciones es más limitada. Aunque esta información pueda ser parte integrante de las investigaciones, es posible que afecte tanto a la intimidad como el contenido de las comunicaciones relativas a las transacciones.

44. Para combatir la financiación del terrorismo y el blanqueo de capitales los Estados han obligado a la industria financiera a analizar las transacciones financieras a fin de distinguir automáticamente entre las "normales" y las "sospechosas". Así, la Unión Europea promulgó en 2005 una directiva sobre la prevención de la utilización del sistema financiero para el blanqueo de capitales y la financiación del terrorismo[65], en la que se pedía a las instituciones financieras que aplicaran las medidas de diligencia debida informando a las unidades de inteligencia financiera (UIF) de las actividades sospechosas y de aquellas sobre las que existieran motivos razonables para sospechar. El tratamiento que las UIF dan a esta información sigue siendo opaco pero Estados como Australia[66] y el Canadá[67] procesan cada año millones de transacciones por medio de instrumentos avanzados de prospección de datos.

45. Las terceras partes pueden estar también sometidas a leyes extranjeras que exijan la revelación. Así, el Gobierno de los Estados Unidos emitió requerimientos administrativos a la Society for Worldwide Interbank Financial Telecommunication (SWIFT), cooperativa belga responsable de permitir el intercambio de mensajes entre más de 7.800 instituciones financieras de más de 200 países. Al obtener acceso al centro de datos de SWIFT en los Estados Unidos, el Departamento del Tesoro del país pudo supervisar las transacciones financieras extranjeras en toda la red SWIFT, encontrar e identificar a terroristas sospechosos[68]. Los grupos de derechos humanos formularon reclamaciones legales en más de 20 tribunales sosteniendo que al entregar esta información a las autoridades de los Estados Unidos SWIFT había violado las leyes locales de intimidad[69].

46. Preocupa también al Relator Especial que la vigilancia se esté introduciendo en las infraestructuras tecnológicas y que éstas generen riesgos a los individuos y las organizaciones. Por ejemplo, el desarrollo de normas para la interceptación legal de las comunicaciones requiere que las compañías de telecomunicación diseñen puntos vulnerables en sus tecnologías que permitan a los Estados interceptar las comunicaciones. De esta posibilidad se sirvieron fraudulentamente terceras partes en Grecia que pudieron escuchar las comunicaciones del Primer Ministro y de docenas de otros altos funcionarios[70].

2008.

[65] Véase la directiva 2005/60/CE del Parlamento Europeo y del Consejo, de 26 de octubre de 2005, sobre la prevención de la utilización del sistema financiero para el blanqueo de capitales y la financiación del terrorismo, *Diario Oficial*, L 309 (2005), págs. 15 a 36.

[66] Véase Australian transaction Reports and Analysis Centre, *AUSTRAC Annual Report 2008-2009*, octubre de 2009.

[67] Véase "Financial Transaction and Reports Analysis Centre of Canada", *FINTRAC Annual Report 2008*, 11 de septiembre de 2008.

[68] Véase también la declaración del Subsecretario de los Estados Unidos Stuart Levey sobre el Programa de seguimiento de la financiación del terrorismo, 23 de junio de 2006.

[69] Véase, por ejemplo, Privacy International, "Pulling a Swift one? Bank transfer information sent to U.S. authorities", 27 de julio de 2006.

[70] Véase, a título informativo, V. Prevelakis y D. Spinellis, "The Athens Affair", *IEEE Spectrum*, julio de 2007.

Más recientemente el Gobierno de la República Islámica del Irán se sirvió de esta posibilidad para vigilar a manifestantes[71]. Para evitar los abusos, las tecnologías de vigilancia deben registrar quién accede a los datos, dejando de esta manera una pista que también se puede seguir para detectar abusos[72].

47. Sin embargo, en algunos Estados se continúan aplicando las garantías constitucionales. En el Canadá, por ejemplo, la Carta de Derechos y Libertades protege la privacidad de la información que obra en manos de terceras partes cuando revela detalles íntimos de la vida y las opciones personales del individuo[73]. Ello requiere equilibrar los intereses de la sociedad en la protección de la dignidad, integridad y autonomía individuales con el cumplimiento efectivo de la ley[74]. De manera análoga, la jurisprudencia del Tribunal Europeo de Derechos Humanos ha extendido el derecho a la intimidad a la información en poder de terceros. El Convenio para la protección de las personas con respecto de la computadorización de datos personales requiere que tanto el sector público como el sector privado protejan la información que poseen y regula el intercambio de información con los organismos del Gobierno. Hay excepciones cuando se trata de proteger la seguridad del Estado, la seguridad pública o los intereses monetarios del Estado, la represión de delitos o la protección del individuo o de los derechos y libertades de los demás[75].

D. Las mejores prácticas

48. Preocupa al Relator la existencia de una tendencia hacia la extensión de los poderes de vigilancia del Estado más allá del terrorismo. Tras los sucesos del 11 de septiembre de 2001 diversas legislaturas introdujeron cláusulas de extinción y revisiones de la legislación antiterrorista pues se supuso se necesitarían poderes extraordinarios durante un corto período de tiempo para responder a ese peligro. Esas cláusulas de extinción y revisiones no se incluyeron en algunas esferas de la actuación política y en las políticas ulteriores no se consideraron en absoluto. Muchos de los poderes de investigación concedidos a las fuerzas de orden público en virtud de leyes antiterroristas se otorgan a esas fuerzas para realizar investigaciones no relacionadas con el terrorismo. Entre tanto los Estados aplican sus propias políticas sin considerar sus efectos en los derechos humanos. Muchas de las políticas descritas más arriba fueron introducidas en principio con carácter extraordinario aunque pronto se convirtieron en normas regionales e internacionales. Colectivamente, esa injerencia tiene un impacto negativo importante en la protección del derecho a la intimidad, al ser limitado el acceso a las salvaguardias legales. Sin un conjunto riguroso de garantías jurídicas y de medios que permitan evaluar la necesidad, proporcionalidad o racionalidad de la injerencia, los Estados carecen de orientación sobre la forma de minimizar el riesgo a la intimidad generado por sus nuevas políticas. El Relator Especial ha determinado las salvaguardias legales que han surgido en el proceso político, la jurisprudencia, el análisis político y las buenas prácticas en todo el mundo.

[71] Véase a título de referencia Nokia Siemens Networks, "Provision of lawful intercept capability in Iran", 22 de junio de 2009.
[72] Véase la nota 54.
[73] Véase Tribunal Supremo del Canadá *R. v. Plant,* 1993 y *R. v. Tessling*, 2004.
[74] *R. v. Plant.*
[75] Artículo 9 del Convenio para la protección de las personas respecto de la computadorización de datos personales.

1. El principio de la intrusión mínima

49. Ciertas injerencias en la vida privada de los ciudadanos son más intrusivas que otras. En los últimos 50 años la protección constitucional de los bienes y las personas se ha extendido con la inclusión de las comunicaciones[76], la información referente a un núcleo biográfico[77] y el derecho a la confidencialidad e integridad de los sistemas de tecnología de la información[78]. Estas protecciones exigen que los Estados hayan agotado sus técnicas menos intrusivas antes de recurrir a las otras. El Comité de Asuntos Internos del Parlamento del Reino Unido examinó y adaptó estas ideas sobre los modernos sistemas de vigilancia centrada en los datos al principio de minimización de los datos, que guarda estrecha relación con la especificación de la finalidad[79]. En su examen, el Comité Parlamentario recomendó que los Gobiernos se resistieran a la tendencia a reunir un volumen mayor de información personal y establecer bases de datos mayores. Toda decisión de crear una nueva base de datos más importante, de intercambiar información sobre bases de datos o de ejecutar propuestas de intensificación de la vigilancia se debería basar en una necesidad demostrada. El Relator Especial sostiene que los Estados deben incorporar este principio a su política actual y futura cuando expliquen la necesidad, y a su vez, la proporcionalidad de su política.

2. El principio de la especificación del fin para limitar utilizaciones secundarias

50. Aunque las leyes de protección de datos deben tratar de que la información obtenida para un fin no se utilice para otro, la política nacional de seguridad y orden público no está sometida por lo general a estas restricciones. La exención se consigue a través de disposiciones de confidencialidad en las notificaciones de acceso legal, órdenes judiciales amplias y certificados de exención tales como los certificados de seguridad nacional, que eximen a una base de datos específica de respetar las leyes que protegen la intimidad. Preocupa al Relator Especial que ello limite la efectividad de las salvaguardias necesarias contra los abusos. Los Estados deben estar obligados a establecer una base legal para la reutilización de información, de acuerdo con los principios constitucionales y de derechos humanos. Ello debe hacerse en el marco de los derechos humanos y no recurriendo a suspensiones y excepciones. Ello es particularmente importante cuando la información se intercambia a través de las fronteras; además, cuando la información se intercambia entre Estados, debe continuar la aplicación de medidas de protección y de salvaguardia[80].

3. El principio de supervisión y autorización regulada del acceso legal

51. Los sistemas de vigilancia requieren una supervisión efectiva que minimice los daños y los abusos. Cuando existen salvaguardias, esta supervisión ha adoptado tradicionalmente la forma de una autorización independiente reflejada en una orden o un proceso judicial con posibilidad de revisión independiente. Sin embargo, muchas políticas han tratado de limitar la supervisión y reducir los niveles de autorización; las leyes de interceptación de las comunicaciones han reducido al mínimo la necesidad de autorización en el caso de ciertas comunicaciones; para acceder a ciertas informaciones en poder de terceros se emiten órdenes judiciales secretas que han limitado la capacidad de recabar

[76] Véase Tribunal Supremo de los Estados Unidos, *Katz v. United States*, 1967.
[77] Véase la nota 74.
[78] Véase la decisión del Tribunal Constitucional de Alemania Nº 370/07, 27 de febrero de 2008.
[79] Véase Comité de Asuntos Interiores del Parlamento del Reino Unido, *A Surveillance Society? Fifth report of the session 2007-2008*, 8 de junio de 2008.
[80] Véase, por ejemplo, con relación a las listas de pasajeros, el artículo 29 de la opinión 8/2004 del Grupo de Trabajo sobre protección de datos, relativo a la información para pasajeros sobre la transferencia de datos del registro de nombres de pasajeros en vuelos entre la Unión Europea y los Estados Unidos de América, 30 de septiembre de 2004.

protección judicial; y los Estado permiten cada vez más a los organismos de inteligencia y las fuerzas de seguridad autoautorizarse a acceder a información personal cuando anteriormente se necesitaba alguna forma de autorización independiente y de información efectiva.

52. Algunos Estados han adoptado medidas para hacer frente a la erosión de las salvaguardias. En los Estados Unidos, tras cierto número de casos judiciales y con consecuencia de las exigencias de reautorización previstas en la *USA Patriot Act*, se han reintroducido nuevas oportunidades de revisión judicial. Los cambios aportados a las prácticas de vigilancia de las comunicaciones en Suecia y los Estados Unidos han reintroducido algunas salvaguardias limitadas en formas de órdenes judiciales. Análogamente, el Tribunal de Justicia de las Comunidades Europeas determinó que los tribunales tenían que examinar la legalidad en el derecho interno de las listas de vigilancia internacional[81].

53. Preocupa al Relator Especial que la falta de un examen efectivo e independiente de las técnicas y prácticas de vigilancia arroje dudas sobre si las injerencias son ilegales (y por consiguiente responsables) y necesarias (y por consiguiente proporcionadas). Elogia la dura labor de los órganos de supervisión de los gobiernos, incluidas las oficinas internas que se ocupan de la intimidad, los departamentos de auditoría y las inspecciones generales, pues también desempeñan un papel fundamental en la determinación de los abusos. Por consiguiente, el Relator Especial pide que aumente la supervisión interna como complemento del proceso de autorización independiente y supervisión externa. Este sistema de responsabilidad interna y externa asegurará la existencia de recursos efectivos a disposición de los individuos, con un acceso significativo a los mecanismos de reparación.

4. El principio de transparencia e integridad

54. La aplicación de privilegios de confidencialidad a los sistemas de vigilancia inhibe la capacidad de los legisladores, los órganos judiciales y el público en general de examinar los poderes del Estado. El individuo puede estar sometido a una vigilancia inadecuada, en la que se elaboran perfiles obtenidos a través de la prospección de datos, y a errores judiciales, sin que haya recibido ninguna notificación precedente de la práctica de que es objeto. Además, la falta de limitaciones claras y adecuadas de la política de vigilancia hace difícil demostrar que esos poderes no se utilizan de manera arbitraria e indiscriminada.

55. El principio de transparencia e integridad requiere la apertura y la comunicación de las prácticas de vigilancia. En algunos Estados existe la obligación de notificar al individuo la vigilancia de que es objeto y la forma en que se ejerce en el momento del hecho o tan pronto como sea posible inmediatamente después. En los regimenes constitucionales de *habeas data* de América Latina[82] y las leyes europeas de protección de datos, los individuos podrán acceder y corregir la información personal que obre en los bancos de datos y en los sistemas de vigilancia. Estos derechos se deberán reconocer más allá de las fronteras garantizando que los regímenes jurídicos protegen tanto a los ciudadanos como a los no ciudadanos.

56. Un debate abierto y un examen minucioso son esenciales para comprender las ventajas y los límites de las técnicas de vigilancia, de forma que el público pueda comprender la necesidad y la legalidad de la vigilancia. En muchos Estados se ha

[81] *Yassin Abdullah Kadi and Barakaat Internation al Foundation v. Council and Commission*, septiembre de 2008.

[82] Véase, por ejemplo, la Constitución del Brasil, art. 5 (LXXI); la Constitución del Paraguay, art. 135; la Constitución de la Argentina, art. 43.

encargado a los Parlamentos y a los órganos independientes la realización de estudios de las políticas y procedimientos de vigilancia y en ocasiones se les ha ofrecido la oportunidad de proceder a un examen prelegislativo. Ello se ha visto facilitado por la utilización de cláusulas de extinción y revisión en la legislación.

5. El principio de la modernización efectiva

57. Aunque es cada vez más fácil obtener mayor información de carácter invasivo, los Estados no han desarrollado una protección proporcional. De hecho, en nombre de la modernización de sus poderes de vigilancia, los Estados han tratado intencionalmente a veces de aplicar sistemas de salvaguardia anticuados y más débiles a informaciones cada vez más sensibles[83]. Conscientes de la necesidad de examinar cómo el cambio político y tecnológico puede influir negativamente en el individuo, algunos Estados han introducido evaluaciones del impacto en la intimidad que articulan dimensiones de privacidad en el diseño de las nuevas técnicas de vigilancia, incluida la forma en que los políticos consideran muchos de los principios expuestos, en particular la minimización de datos y el derecho a una reparación. El Relator Especial cree que el uso de instrumentos tales como la evaluación del impacto en la intimidad pueden contribuir a informar al público de las prácticas de vigilancia e instilar al mismo tiempo una cultura de la intimidad en los órganos del gobierno que elaboran nuevos sistemas de vigilancia para combatir el terrorismo. Se deben asimismo adoptar normas internacionales que exijan a los Estados que aumenten sus salvaguardias para reflejar el cambio tecnológico.

IV. Conclusiones y recomendaciones

A. Conclusiones

58. **Preocupa al Relator Especial que lo que antaño era excepcional sea hogaño habitual. En primer lugar los Estados han dejado de limitar los sistemas excepcionales de vigilancia a la lucha contra el terrorismo para dedicarlos a toda clase de finalidades. En segundo lugar, la vigilancia ha pasado a formar parte de la política. Los críticos de las propuestas de vigilancia extrajudicial deben ahora centrarse en las razones por las que no se debe obtener información adicional pues el Estado ya no tiene la obligación de demostrar que la injerencia es necesaria. En tercer lugar se ha reducido la calidad y la efectividad de prácticamente todos los dispositivos legales de protección y salvaguardia. Ello sucede incluso en una época en que el cambio tecnológico permite unos poderes de vigilancia mayores y más invasivos. Sin embargo, más preocupante es que todas estas tecnologías y políticas se exportan a otros países y con frecuencia pierden en el proceso incluso las protecciones más básicas.**

59. **Es necesario elaborar normas jurídicas internacionales de protección contra estas formas de abuso. Ello se vería facilitado por la adhesión a los principios descritos en el presente informe, garantizando en particular que la vigilancia es lo menos intrusiva posible y que se han establecido los nuevos poderes con las salvaguardias y limitaciones adecuadas, la autorización y supervisión efectivas y el examen y la información regulares sobre los mismos, y que van acompañados de declaraciones amplias sobre su impacto en la intimidad. Los poderes legislativos y el público en general han tenido rara vez la oportunidad de discutir si los mecanismos antiterroristas son necesarios, proporcionales o razonables. El Relator Especial cree**

[83] Véase the Policiy Engagement Network, *Briefing on the UK Government's Interception Modernisation Programme*, junio de 2009.

que las buenas prácticas emergentes que se describen a continuación pueden resultar beneficiosas para todos.

B. Recomendaciones

A las asambleas legislativas

60. **El Relator Especial recomienda una vez más que toda injerencia en la vida privada, la familia, el domicilio o la correspondencia sea autorizada en virtud de disposiciones legislativas que sean de conocimiento público, particularmente precisas y proporcionales a la amenaza contra la seguridad y por otras garantías efectivas contra el abuso. Los Estados deben asegurarse de que las autoridades competentes aplican métodos de investigación menos intrusivos si dichos métodos permiten detectar, prevenir o perseguir con eficacia suficiente los delitos de terrorismo. Las autoridades decisorias deben estar estructuradas de forma que cuanto mayor sea la invasión de la intimidad más alto sea el nivel de autorización necesario.**

61. **La adhesión a las normas internacionales de protección de la intimidad y de derechos humanos debe ser un principio del derecho interno. Por consiguiente, es necesaria una ley general de la intimidad y la protección de datos que garantice la existencia de disposiciones legislativas claras de protección del individuo que impidan la obtención excesiva de información personal, asegure la existencia de medidas que garanticen la veracidad de la información, establezca límites sobre el uso, almacenamiento e intercambio de la información y prescriba que se notifique a los individuos la forma en que se utiliza la información sobre ellos y su derecho de acceso y reparación, con independencia de su nacionalidad y jurisdicción.**

62. **Se deben establecer mandatos de supervisión estrictos e independientes para examinar las políticas y prácticas a fin de garantizar la existencia de una rigurosa supervisión del uso de técnicas intrusivas de vigilancia y del procesamiento de la información personal. Por consiguiente no debe haber ningún sistema secreto de vigilancia que no se encuentre sometido al examen de un órgano de supervisión efectivo y todas las injerencias deben ser autorizadas por un órgano independiente.**

63. **Las políticas antiterroristas actuales y propuestas deben incluir evaluaciones de su efecto en la intimidad que permitan examinar y comunicar la forma en que la política y la tecnología garantiza la mitigación de las amenazas de la intimidad y la consideración de la intimidad en las primeras fases de elaboración de la política.**

64. **El Relator Especial recomienda que se elaboren salvaguardias más sólidas que garanticen que el intercambio de información entre gobiernos continúa protegiendo la intimidad privada.**

65. **El Relator Especial recomienda también que se elaboren normas más estrictas que limiten el acceso de los gobiernos a la información en poder de terceros, incluidos los sistemas de presentación de informes, y que minimicen la carga que pesa sobre terceras partes de reunir información adicional y que se apliquen las salvaguardias legales y constitucionales cuando actúan terceras partes en nombre del Estado.**

66. **El Relator Especial advierte de la necesidad de reconsiderar el lenguaje legislativo si se quiere evitar la utilización de los poderes antiterroristas con otras finalidades. Se deben diseñar nuevos sistemas con una limitación de ámbito claramente especificada.**

A los gobiernos

67. **El Relator Especial insta a los gobiernos a que expliquen detalladamente cómo sus políticas de vigilancia se ajustan a los principios de proporcionalidad y necesidad, de conformidad con las normas internacionales de derechos humanos y qué medidas han tomado para prevenir abusos.**

68. **El Relator Especial recomienda una discusión abierta y una información regular sobre los programas de vigilancia basados en la información. Los informes destinados a los órganos legislativos y de supervisión y el examen independiente de las prácticas contribuirán a informar la política futura y las deliberaciones sobre la política antiterrorista.**

69. **Todo programa de vigilancia basado en listas o en perfiles deberá incluir las debidas garantías procesales para todos los individuos, en particular el derecho de reparación. Se debe mantener el principio de transparencia de forma que los individuos sean informados de cómo y porqué fueron incluidos en listas de vigilancia y de cómo se elaboró su perfil, y de los mecanismo de recurso sin cargas indebidas.**

70. **Dados los peligros inherentes a la prospección de datos, el Relator Especial recomienda que todo el programa de lucha contra el terrorismo basado en la información sea sometido a una supervisión estricta e independiente. El Relator Especial formula asimismo una recomendación en contra de la elaboración y utilización de técnicas de prospección de datos con fines antiterroristas.**

71. **A la luz del riesgo de uso indebido de las tecnologías de vigilancia, el Relator Especial recomienda que se dedique una cantidad igual de recursos de investigación y desarrollo a las tecnologías de promoción de la intimidad.**

Al Consejo de Derechos Humanos

72. **El Relator Especial recomienda la elaboración de un programa de creación de capacidad mundial en materia de protección de la intimidad. La multiplicación internacional de leyes antiterroristas y de normas mundiales sobre vigilancia debe ser contrapesada con un mayor conocimiento de las salvaguardias necesarias para la protección de la dignidad del individuo.**

73. **El Relator Especial exhorta al Consejo de Derechos Humanos a que establezca un proceso que se base en los principios existentes de protección de datos para recomendar medidas para la creación de una declaración mundial sobre la protección y el carácter secreto de los datos.**

Al Comité de Derechos Humanos

74. **El Relator Especial recomienda al Comité de Derechos Humanos que comience a redactar una nueva observación general sobre el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos con el objeto de elaborar una prueba adecuada de la limitación, proporcionando de esta manera orientación a los Estados sobre las salvaguardias apropiadas. La observación general debe asimismo prestar la debida atención a la protección de datos como atributo del derecho a la intimidad, recogido en el artículo 17 del Pacto.**