



UNODC

Oficina de las Naciones Unidas
contra la Droga y el Delito



El uso de internet con fines terroristas

En colaboración con el
EQUIPO ESPECIAL SOBRE LA EJECUCIÓN DE LA LUCHA CONTRA EL TERRORISMO

OFICINA DE LAS NACIONES UNIDAS CONTRA LA DROGA Y EL DELITO
Viena

EL USO DE INTERNET CON FINES TERRORISTAS



NACIONES UNIDAS
Nueva York, 2013

© Naciones Unidas, julio de 2013. Reservados todos los derechos a nivel mundial.

Las denominaciones empleadas en la presente publicación y la forma en que aparecen los datos que contiene no implican de parte de la Secretaría de las Naciones Unidas juicio alguno sobre la condición jurídica de ninguno de los países, territorios, ciudades o zonas citados, o de sus autoridades, ni respecto del trazado de sus fronteras o límites.

La información acerca de localizadores uniformes de recursos y de enlaces con sitios de Internet contenida en la presente publicación se brinda para comodidad del lector y es correcta en la fecha de publicación. Las Naciones Unidas no asumen ninguna responsabilidad por la exactitud de dicha información después de esa fecha ni por el contenido de ningún sitio web externo.

Producción editorial: Sección de Servicios en Inglés, Publicaciones y Biblioteca, Oficina de las Naciones Unidas en Viena.

“Internet es un excelente ejemplo de cómo los terroristas pueden actuar de manera verdaderamente transnacional. En respuesta a ello, los Estados deben pensar y funcionar de manera igualmente transnacional”.

Ban Ki-moon
Secretario General de las Naciones Unidas

Prólogo

Director Ejecutivo Oficina de las Naciones Unidas contra la Droga y el Delito

El uso de Internet con fines terroristas es un fenómeno que se propaga con rapidez y exige una respuesta dinámica y coordinada de los Estados Miembros.

La Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) desempeña un papel clave en la prestación de asistencia a los Estados Miembros, en cumplimiento de su mandato de fortalecer la capacidad de los sistemas nacionales de justicia penal para aplicar las disposiciones de los instrumentos jurídicos internacionales contra el terrorismo, y lo hace de conformidad con los principios del estado de derecho y las normas internacionales de derechos humanos. En particular, en 2011 la Asamblea General, en su resolución 66/178, reafirmó el mandato de la UNODC de seguir desarrollando los conocimientos jurídicos especializados en el campo de la lucha contra el terrorismo y en las esferas temáticas pertinentes, incluido el uso de Internet con fines terroristas.

Pese a que en los últimos años se viene reconociendo cada vez más la amenaza que representa el uso de Internet por los terroristas, actualmente no existe ningún instrumento universal que se refiera específicamente a ese aspecto generalizado de la actividad terrorista. Además, hay pocos programas de capacitación especializada en los aspectos jurídicos y prácticos de la investigación y el enjuiciamiento de casos de terrorismo en que se haya usado Internet. La presente publicación complementa la documentación existente preparada por la UNODC en las esferas de la lucha contra el terrorismo y el delito cibernético, y el estado de derecho. Asimismo, aborda la importancia de desarrollar un conocimiento integrado y especializado para responder a las necesidades de asistencia técnica de los Estados Miembros en la lucha contra esta amenaza en permanente evolución. La UNODC está profundamente agradecida por el generoso apoyo prestado por el Gobierno del Reino Unido de Gran Bretaña e Irlanda del Norte, que hizo posible la publicación de esta obra.

La publicación, concebida para su utilización como recurso independiente y como apoyo a las iniciativas de la UNODC de creación de capacidad, tiene el fin de ofrecer orientación acerca de los marcos jurídicos y la práctica actuales en los planos nacional e internacional en cuanto a la penalización, la investigación y el enjuiciamiento de casos de uso de Internet con fines terroristas.

El terrorismo, en todas sus manifestaciones, nos afecta a todos. El uso de Internet para promover fines terroristas va más allá de las fronteras nacionales, lo que amplifica el efecto potencial sobre las víctimas. La presente publicación, al poner de relieve casos concretos y las mejores prácticas para hacer frente a este reto singular, procura lograr dos objetivos: en primer lugar, promover una mejor comprensión de todas las formas en que se puede hacer un uso indebido de las tecnologías de las comunicaciones para promover actos de terrorismo y, en segundo lugar, estrechar la colaboración entre los Estados Miembros, a fin de idear respuestas eficaces de la justicia penal a este reto transnacional.

Yury Fedotov
Director Ejecutivo
Oficina de las Naciones Unidas contra la Droga y el Delito

Equipo Especial sobre la Ejecución de la Lucha contra el Terrorismo del Secretario General

El Grupo de Trabajo sobre medidas para hacer frente al uso de Internet con fines terroristas, del Equipo Especial sobre la Ejecución de la Lucha contra el Terrorismo, tiene por objeto coordinar las actividades del sistema de las Naciones Unidas en apoyo de la Estrategia Global de las Naciones Unidas contra el Terrorismo, aprobada por la Asamblea General en su resolución 60/288, en la que los Estados Miembros decidieron “coordinar los esfuerzos en los planos internacional y regional para combatir el terrorismo en todas sus formas y manifestaciones en Internet” y “utilizar Internet como instrumento para luchar contra la propagación del terrorismo, y al mismo tiempo reconocer que los Estados podrían necesitar asistencia a este respecto”. El Grupo de Trabajo ha señalado tres temas clave para su examen: cuestiones jurídicas, cuestiones técnicas y formas en que la comunidad internacional podría utilizar Internet más eficazmente para combatir el terrorismo poniendo en descubierto la falacia del mensaje terrorista de que la violencia es una forma legítima de lograr el cambio político.

El presente estudio, preparado por la Oficina de las Naciones Unidas contra la Droga y el Delito y llevado a cabo en el marco del Grupo de Trabajo, se realizó en gran medida gracias a la contribución y al apoyo de los Estados Miembros. En él se lleva el examen de los problemas jurídicos a una nueva etapa y se hace una valiosa contribución a los conocimientos y la experiencia que el Grupo de Trabajo ha acumulado y compartido con los Estados Miembros en este ámbito. En particular, proporciona ejemplos importantes de la legislación de los Estados Miembros relativa al uso de Internet por terroristas y demuestra, por medio de ejemplos de casos judiciales reales, las dificultades que enfrentan los Estados Miembros para penalizar y enjuiciar tales actos.

El Grupo de Trabajo confía en que el presente informe contribuirá a determinar qué ámbitos legislativos son los que más se prestan para que las Naciones Unidas asistan a los Estados Miembros en la aplicación de la Estrategia Global contra el Terrorismo para combatir el uso de Internet con fines terroristas.

Richard Barrett
Coordinador del Equipo encargado de prestar apoyo analítico y vigilar la aplicación
de las sanciones
Copresidente del Grupo de Trabajo sobre medidas para hacer frente al uso de
Internet con fines terroristas del Equipo Especial sobre la Ejecución de la Lucha
contra el Terrorismo

Gobierno del Reino Unido

El Reino Unido, uno de los primeros países que promulgaron legislación en la última década para combatir el uso de Internet con fines terroristas, ha tenido un éxito considerable en la lucha contra las actividades terroristas en línea dentro de sus fronteras, a la vez que hemos hecho todo lo posible para defender las libertades y los beneficios que Internet ha traído a sus ciudadanos.

Sin embargo, reconocemos que la amenaza es transnacional por naturaleza. Solo actuando de consuno podrán los miembros de la comunidad internacional aspirar a reprimir el uso terrorista de Internet de forma eficaz.

El Gobierno británico, por tanto, acogió con satisfacción la oportunidad de apoyar a la UNODC en la preparación de la presente publicación. Esperamos que se convierta rápidamente en una herramienta útil para los legisladores, los funcionarios encargados de hacer cumplir la ley y los profesionales de la justicia penal, para desarrollar y aplicar los marcos jurídicos que permitan desbaratar de manera eficaz las actividades terroristas en línea. De ser así, se habrá hecho una valiosa contribución hacia el objetivo de que nuestras comunidades, tanto la real como la virtual, sean lugares más seguros.

Simon Shercliff

Jefe, Departamento de Lucha contra el Terrorismo (OPS), Oficina de Relaciones Exteriores y del Commonwealth

Sue Hemming OBE

Jefe de la División Especial de lucha contra el terrorismo y la delincuencia Fiscalía del Estado

Índice

	<i>Página</i>
Prólogo	v
Director Ejecutivo Oficina de las Naciones Unidas contra la Droga y el Delito.	v
Equipo Especial sobre la Ejecución de la Lucha contra el Terrorismo del Secretario General	vi
Gobierno del Reino Unido	vii
Antecedentes	1
I. El uso de Internet con fines terroristas	3
A. Introducción.	3
B. Uso de Internet con fines terroristas: medios empleados	3
C. Uso de Internet para combatir las actividades terroristas	13
D. Consideraciones fundadas en el estado de derecho.	14
II. El contexto internaciona.	17
A. Introducción.	17
B. Resoluciones de las Naciones Unidas contra el terrorismo.	18
C. Instrumentos jurídicos universales contra el terrorismo.	19
D. Normas jurídicas internacionales de derechos humanos	21
E. Instrumentos jurídicos regionales y subregionales contra el terrorismo	22
F. Legislación modelo	26
III. Marcos normativo y legislativo.	29
A. Introducción.	29
B. Políticas	29
C. Legislación	33
IV. Investigaciones y reunión de inteligencia.	57
A. Recursos que ofrece Internet para la comisión de delitos terroristas.	57
B. Investigaciones de casos de terrorismo en que se usó Internet.	65

	<i>Página</i>
C. Técnicas forenses de preservación y recuperación de datos	69
D. Validación de la autenticidad de las pruebas digitales.	72
E. Dependencias operacionales de lucha contra la ciberdelincuencia. . .	73
F. Reunión de inteligencia	75
G. Formación	78
V. Cooperación internacional.	81
A. Introducción.	81
B. Instrumentos y acuerdos de cooperación internacional	81
C. Marcos legislativos nacionales	92
D. Otras medidas fuera de las legislativas.	92
E. Cooperación oficial y oficiosa	98
F. Dificultades y problemas	101
VI. El proceso penal.	111
A. Introducción.	111
B. Enfoque del proceso penal basado en el estado de derecho	111
C. Función del fiscal en los casos de terrorismo	112
D. Fase de la investigación	114
E. Cooperación internacional	116
F. Fase acusatoria.	117
G. Fase del juicio: cuestiones probatorias.	118
H. Otras cuestiones.	132
VII. Cooperación del sector privado.	135
A. Función de los interesados del sector privado.	135
B. Asociaciones entre el sector público y el privado	143
VIII. Conclusiones.	147
A. Uso de Internet con fines terroristas.	147
B. Contexto internacional.	147
C. Marcos normativo y legislativo	148

	<i>Página</i>
D. Investigaciones y reunión de datos de inteligencia.	150
E. Cooperación internacional	151
F. El proceso penal	154
G. Cooperación del sector privado	157

Antecedentes

La tecnología es uno de los factores estratégicos que llevan a las organizaciones terroristas y sus partidarios a hacer un mayor uso de Internet con una gran variedad de propósitos, incluidos el reclutamiento, la financiación, la propaganda, el adiestramiento, la incitación a cometer actos de terrorismo, y la reunión y difusión de información con fines terroristas. Aunque Internet brinda numerosos beneficios que son evidentes, también puede utilizarse para facilitar la comunicación dentro de las organizaciones terroristas y para transmitir información sobre planes de actos terroristas, así como para prestar apoyo material a esos planes, todo lo cual significa que se necesitan conocimientos técnicos específicos para la investigación eficaz de esos delitos.

Es un principio comúnmente aceptado que los presuntos terroristas, a pesar de la naturaleza atroz de sus actos, deben gozar de las mismas garantías procesales penales que cualquier otro sospechoso. La defensa de los derechos humanos es un valor fundamental de las Naciones Unidas y la piedra angular del enfoque del estado de derecho de la lucha contra el terrorismo. En la presente publicación se destaca, por consiguiente, la importancia del respeto de los principios de los derechos humanos y las libertades fundamentales en todo momento y, en particular, en el contexto del desarrollo y la aplicación de los instrumentos jurídicos relativos a la lucha contra el terrorismo.

La Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), una de las principales entidades de las Naciones Unidas que prestan asistencia jurídica y técnica conexa en la lucha contra el terrorismo, participa activamente en la labor del Equipo Especial sobre la Ejecución de la Lucha contra el Terrorismo, asegurando así que su propia labor se integre en el contexto más amplio de las actividades de todo el sistema de las Naciones Unidas y se coordine con todas ellas. En enero de 2010, el Equipo Especial del Grupo de Trabajo sobre medidas para hacer frente al uso de Internet con fines terroristas inició una serie de conferencias en que participaron representantes de los gobiernos, organizaciones internacionales y regionales, grupos de estudio, instituciones académicas y entidades del sector privado para evaluar el uso de Internet con fines terroristas y los posibles medios de contrarrestar ese uso. El objetivo de la iniciativa del Grupo de Trabajo era proporcionar a los Estados Miembros información general sobre la naturaleza actual del problema y proponer directrices de política, proyectos y orientación práctica sobre los aspectos jurídicos, técnicos y de presentación de argumentos contra el terrorismo. El Grupo de Trabajo celebró conferencias en Berlín en enero de 2010, en Seattle (Estados Unidos de América) en febrero de 2010 y en Riad en enero de 2011.

En cumplimiento de su mandato de seguir “desarrollando conocimientos jurídicos especializados en el campo de la lucha contra el terrorismo ... y proporcionando asistencia a los Estados Miembros que la soliciten con respecto a las respuestas de la justicia

penal al terrorismo, incluidos ... la utilización de Internet con fines terroristas”¹, la Subdivisión de Prevención del Terrorismo de la UNODC, en colaboración con la Subdivisión de Lucha contra la Delincuencia Organizada y el Tráfico Ilícito de la UNODC y con el apoyo del Gobierno del Reino Unido de Gran Bretaña e Irlanda del Norte, se comprometió a contribuir al proyecto del Grupo de Trabajo mediante el perfeccionamiento del actual instrumento de asistencia técnica contra la utilización de Internet con fines terroristas. La publicación actual de la UNODC se basa en las conclusiones de las conferencias del Grupo de Trabajo y, en particular, la conferencia celebrada en Berlín en enero de 2010, sobre las cuestiones jurídicas del terrorismo relacionadas específicamente con Internet.

En relación con la preparación de la presente publicación, la UNODC organizó dos reuniones de grupos de expertos en Viena, en octubre de 2011 y febrero de 2012, a fin de proporcionar un foro para que los especialistas en la lucha contra el terrorismo, provenientes de un grupo de Estados Miembros diverso desde el punto de vista geográfico, intercambiaran sus experiencias en relación con la lucha contra el uso de Internet con fines terroristas. Participaron en estas reuniones expertos de un total de 25 Estados Miembros, incluidos fiscales superiores, funcionarios encargados de hacer cumplir la ley, y miembros de la comunidad académica, así como representantes de varias organizaciones intergubernamentales. La presente publicación se basa en gran medida en los debates y los conocimientos especializados compartidos durante esas reuniones y tiene por objeto ofrecer orientación práctica a los Estados Miembros para facilitar la investigación y el enjuiciamiento más eficaces de casos de terrorismo que entrañen el uso de Internet.

I. El uso de Internet con fines terroristas

A. Introducción

1. Desde finales de la década de 1980, Internet ha demostrado ser un medio de comunicación sumamente dinámico, que llega a un público cada vez mayor en todo el mundo. El desarrollo de tecnologías cada vez más sofisticadas ha creado una red con un alcance verdaderamente mundial y barreras al acceso relativamente bajas. La tecnología de Internet hace que resulte fácil para una persona comunicarse con relativo anonimato, rapidez y eficacia, a través de las fronteras, con un público casi ilimitado. Los beneficios de la tecnología de Internet son numerosos, comenzando por la facilidad singular con que se comparten información e ideas, lo que está reconocido como derecho humano fundamental². Sin embargo, cabe reconocer que la misma tecnología que facilita dicha comunicación puede explotarse también con fines terroristas. El uso de Internet con fines terroristas crea oportunidades y desafíos en la lucha contra el terrorismo.

B. Uso de Internet con fines terroristas: medios empleados

2. A los efectos de la presente publicación, se ha adoptado un enfoque funcional en relación con la clasificación de los medios por los cuales se suele utilizar Internet para promover los actos de terrorismo y prestarles apoyo. Este enfoque ha dado lugar a la clasificación de seis categorías que suelen superponerse, a saber: la propaganda (incluidos el reclutamiento, la radicalización y la incitación al terrorismo); la financiación; el adiestramiento; la planificación (tanto por medio de comunicaciones secretas, como mediante la información de dominio público); la ejecución; y los ataques cibernéticos. A continuación se examina cada una de esas categorías con mayor detalle.

1. *Propaganda*

3. Uno de los principales usos de Internet por los terroristas es la difusión de propaganda. Esta generalmente adopta la forma de comunicaciones de audio y video, que imparten instrucción ideológica o práctica, dan explicaciones y justificaciones o promueven actividades terroristas. El material puede consistir en mensajes, presentaciones, revistas, tratados, ficheros de video y audio virtuales, y en juegos de video elaborados por organizaciones terroristas o sus simpatizantes. No obstante, la determinación de

²Véase, por ejemplo, el Pacto Internacional de Derechos Civiles y Políticos (resolución 2200 A (XXI), de la Asamblea General (anexo)), art. 19, párr. 2.

qué es lo que constituye propaganda terrorista y no promoción legítima de un punto de vista suele ser una evaluación subjetiva. Además, la difusión de propaganda no es generalmente, en sí y de por sí, una actividad prohibida. Uno de los principios básicos del derecho internacional es la protección de los derechos humanos fundamentales, que incluyen el derecho a la libertad de expresión (véase el análisis del tema en la sección I. D, *infra*). Esto garantiza a las personas el derecho de compartir una opinión o distribuir contenido que puede ser considerado ofensivo por otros, a reserva de ciertas excepciones limitadas. Una exclusión generalmente aceptada con respecto a ese derecho es la prohibición de la distribución de ciertas categorías de contenido sexualmente explícito, por considerarse de interés público el proteger a determinados grupos vulnerables. Otras excepciones, que deben estar previstas por ley y cuya necesidad debe haberse demostrado, pueden incluir las comunicaciones que son claramente perjudiciales para la protección de la seguridad nacional, y las que puedan tener por fin incitar a la comisión de actos de violencia contra personas o grupos específicos de personas y tengan probabilidades de lograrlo³.

4. La promoción de la violencia es un tema común de la propaganda relacionada con el terrorismo. El amplio alcance de los contenidos distribuidos por Internet aumenta exponencialmente el público que puede verse afectado. Además, la capacidad de distribuir directamente el contenido a través de Internet disminuye la dependencia de los canales tradicionales de comunicación, como los servicios de noticias, que pueden tomar medidas para evaluar de forma independiente la credibilidad de la información recibida, o para modificar o suprimir los aspectos que se consideren excesivamente provocativos. La propaganda por Internet también puede incluir contenidos como imágenes de video de actos de violencia de terrorismo o juegos de video, creados por organizaciones terroristas, que simulan actos de terrorismo y alientan al usuario a participar en el juego de rol, haciendo el papel de terrorista virtual.

5. La promoción de la retórica extremista, que fomenta los actos de violencia, también es una tendencia común en toda la gama, cada vez mayor, de plataformas basadas en Internet que hospedan contenido generado por los usuarios. Contenidos que antes podrían haber sido distribuidos a un público relativamente limitado, en persona o a través de medios físicos como discos compactos (CD) y discos de video digital (DVD), han ido pasando cada vez más hacia Internet. Los contenidos pueden distribuirse ahora usando una amplia gama de herramientas, tales como sitios web especiales, salas virtuales de charla y foros, revistas en línea, plataformas de redes sociales como Twitter y Facebook, y sitios web populares de videos y de intercambio de ficheros como YouTube y Rapidshare, respectivamente. El uso de los servicios de indización, como los buscadores de Internet, también hace que sea más fácil descubrir y obtener contenido relacionado con el terrorismo.

6. La amenaza fundamental de la propaganda terrorista se relaciona con la manera en que se utiliza y la intención con que se difunde. Distribuida a través de Internet, la propaganda terrorista abarca toda una gama de objetivos y públicos. Puede estar

concebida especialmente, entre otras cosas, para los partidarios u opositores, posibles o reales, de una organización, o para públicos de creencias extremistas compartidas, o para las víctimas directas o indirectas de los actos de terrorismo o para la comunidad internacional o un subconjunto de esta. La propaganda destinada a partidarios posibles o reales puede centrarse en el reclutamiento, la radicalización y la incitación al terrorismo, mediante mensajes en que se comunica orgullo, sentimientos de triunfo y dedicación al logro de objetivos extremistas. También puede utilizarse para demostrar la ejecución eficaz de los ataques terroristas a quienes han prestado apoyo financiero. Otros objetivos de la propaganda terrorista pueden incluir el uso de la manipulación psicológica para socavar la creencia de las personas en ciertos valores sociales colectivos, o propagar un sentido de gran ansiedad, miedo o pánico en una población o un sector de esta. Esto se puede lograr mediante la difusión de información falsa, rumores, amenazas de violencia o imágenes de actos que llevan a la violencia. Los destinatarios pueden incluir las personas que ven el contenido directamente, así como los afectados por la posible publicidad generada por dicho material. Con respecto a la comunidad internacional en general, el objetivo es a menudo transmitir el deseo de lograr nobles fines políticos⁴.

a) *Reclutamiento*

7. Internet puede utilizarse no solo como un medio para publicar mensajes y videos extremistas, sino también como una forma de establecer relaciones con las personas más receptivas a la propaganda y solicitarles apoyo. Las organizaciones terroristas usan, cada vez con más frecuencia, la propaganda distribuida a través de plataformas tales como sitios web protegidos por contraseña y salas de charla de Internet de acceso restringido como medio de reclutamiento clandestino⁵. El alcance de Internet proporciona a las organizaciones terroristas y simpatizantes un semillero mundial de reclutas potenciales. Los ciberforos de acceso restringido ofrecen a los reclutas un lugar para enterarse de la existencia de organizaciones terroristas y prestarles apoyo, así como para participar en acciones directas en pos de objetivos terroristas⁶. El uso de barreras tecnológicas al acceso a las plataformas de reclutamiento también aumenta la complejidad del rastreo de las actividades relacionadas con el terrorismo por los agentes de los servicios de inteligencia y las fuerzas del orden.

8. La propaganda terrorista suele adaptarse para atraer a los grupos vulnerables y marginados de la sociedad. El proceso de reclutamiento y radicalización comúnmente explota los sentimientos de injusticia, exclusión o humillación⁷. La propaganda puede ser adaptada para tener en cuenta factores demográficos, como la edad o el género, así como las circunstancias sociales o económicas.

⁴Gabriel Weimann, *Terror on the Internet: The New Arena, the New Challenges* (Washington, D.C. Instituto de la Paz de los Estados Unidos, 2006), págs. 37 y 38.

⁵Scott Gerwehr y Sarah Daly, "Al-Qaida: terrorist selection and recruitment", en *The McGraw-Hill Homeland Security Handbook*, David Kamien, ed. (Nueva York, McGraw-Hill, 2006), pág. 83.

⁶Dorothy E. Denning, "Terror's web: how the Internet is transforming terrorism", en *Handbook of Internet Crime*, Yvonne Jewkes y Majid Yar, eds. (Cullompton, Reino Unido, Willan Publishing, (2010)), págs. 194 a 213.

⁷Comisión Europea, Grupo de expertos en materia de radicalización violenta, "Radicalisation processes leading to acts of terrorism" (2008). Puede consultarse en www.clingendael.nl/publications/2008/20080500_cscp_report_vries.pdf.

9. Internet puede ser un medio particularmente eficaz para el reclutamiento de menores de edad, que representan una gran proporción de los usuarios. La propaganda difundida a través de Internet con objeto de reclutar a menores puede tomar la forma de dibujos animados, videos de música popular o juegos de computadora. Entre las tácticas empleadas por los sitios web mantenidos por organizaciones terroristas o sus afiliados para llegar a los menores cabe mencionar el uso de dibujos animados combinados con cuentos infantiles y mensajes que promueven y glorifican los actos de terrorismo, como los atentados suicidas. Del mismo modo, algunas organizaciones terroristas han diseñado juegos de video en línea destinados a ser utilizados como herramientas de reclutamiento y adiestramiento. Estos juegos pueden promover el uso de la violencia contra un Estado o una figura política prominente, premiando los éxitos virtuales, y pueden ofrecerse en varios idiomas para atraer a un público más amplio⁸.

b) *Incitación*

10. Mientras que la propaganda en sí, en general, no está prohibida, muchos Estados Miembros consideran que el uso de propaganda por terroristas para incitar a cometer actos de terrorismo es ilegal. Internet ofrece material y oportunidades en abundancia para descargar, editar y distribuir contenido que podría considerarse una glorificación ilegal de los actos de terrorismo o una incitación a cometerlos. Cabe señalar, empero, que algunas entidades intergubernamentales y de derechos humanos han expresado dudas de que el concepto de “glorificación” del terrorismo sea lo suficientemente restringido y preciso como para servir de base a sanciones penales acordes con las exigencias del principio de legalidad y las limitaciones permisibles del derecho a la libertad de expresión, consagrado en los artículos 15 y 19 del Pacto Internacional de Derechos Civiles y Políticos^{9,10}.

11. Es importante hacer hincapié en la distinción entre mera propaganda y material destinado a incitar a cometer actos de terrorismo. En varios Estados Miembros, para poder considerar a alguien responsable de incitación al terrorismo, es preciso demostrar la intención necesaria y un nexo causal directo entre la supuesta propaganda y un complot real o la ejecución de un acto terrorista. Por ejemplo, en una contribución a las reuniones del grupo de expertos, un experto francés indicó que la difusión de materiales didácticos sobre explosivos no se consideraría una violación del derecho francés a menos que la comunicación contuviera información que especificase que el material se compartía con una finalidad terrorista.

12. La prevención y disuasión de la incitación al terrorismo a fin de proteger la seguridad nacional y el orden público son razones legítimas para limitar la libertad de

⁸Gabriel Weimann, “Online terrorists prey on the vulnerable”, *YaleGlobal Online*, 5 de marzo de 2008. Puede consultarse en <http://yaleglobal.yale.edu/content/online-terrorists-prey-vulnerable>.

⁹Resolución 2200 A (XXI) de la Asamblea General, anexo.

¹⁰Véanse los siguientes informes del Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo: A/65/258 (párr. 46) y A/61/267 (párr. 7); véase también el informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, adición a la Declaración conjunta en el décimo aniversario: Los diez principales desafíos a la libre expresión en la próxima década (A/HRC/14/23/Add.2).

expresión, según lo dispuesto en el artículo 19, párrafo 3, del Pacto Internacional de Derechos Civiles y Políticos. Estas razones son también compatibles con el artículo 20, párrafo 2, de dicho Pacto, que obliga a los Estados a prohibir toda apología del odio nacional, racial o religioso que constituya incitación a la discriminación, la hostilidad o la violencia. Sin embargo, teniendo en cuenta el carácter fundamental del derecho a la libertad de expresión, toda restricción al ejercicio de este derecho debe ser a la vez necesaria y proporcional a la amenaza que representa. El derecho a la libertad de expresión también está vinculado a otros derechos importantes, incluidos los derechos a la libertad de pensamiento, de conciencia y de religión, creencia y opinión¹¹.

c) Radicalización

13. El reclutamiento, la radicalización y la incitación al terrorismo pueden considerarse como puntos a lo largo de un continuo. La radicalización se refiere principalmente al proceso de adoctrinamiento que suele acompañar a la transformación de los reclutas en personas decididas a actuar con violencia, inspiradas por ideologías extremistas. El proceso de radicalización a menudo implica el uso de propaganda, ya sea comunicada en persona o por Internet, en el curso del tiempo. La duración del proceso y la eficacia de la propaganda y otros medios de persuasión empleados pueden variar según las circunstancias y relaciones de cada caso particular.

2. Financiación

14. Las organizaciones terroristas y sus partidarios también pueden usar Internet para financiar actos de terrorismo. La manera en que los terroristas utilizan Internet para recaudar fondos y recursos puede clasificarse en cuatro categorías generales: la recaudación directa, el comercio electrónico, el empleo de los servicios de pago en línea y las contribuciones a organizaciones benéficas. La recaudación directa se lleva a cabo utilizando los sitios web y las salas de charla, las campañas masivas de correo y las comunicaciones dirigidas a simpatizantes para solicitar donaciones. Los sitios web también pueden ser usados como tiendas en línea que ofrecen libros, grabaciones de audio y de video y otros artículos a los simpatizantes. Los servicios de pago en línea que ofrecen algunos sitios web o plataformas de comunicación especiales permiten la transferencia electrónica de fondos entre las partes. Estas transferencias de fondos suelen hacerse por transferencia bancaria electrónica, tarjeta de crédito o servicios de pago alternativos ofrecidos por servicios como PayPal o Skype.

15. Los servicios de pago en línea también pueden ser explotados por medios fraudulentos como el robo de identidad o de tarjetas de crédito, el uso fraudulento de las telecomunicaciones, el fraude bursátil, los delitos contra la propiedad intelectual y el fraude en subastas. Un ejemplo del uso de ganancias ilícitas para financiar actos de terrorismo es la causa del Reino Unido contra Younis Tsouli (véase el párrafo 114 *infra*). Los beneficios producto del robo de tarjetas de crédito fueron blanqueados por varios

¹¹ Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, "Los derechos humanos, el terrorismo y la lucha contra el terrorismo", Folleto informativo núm. 32 (Ginebra, 2008), Cap. III, secc. H.

medios, incluida la transferencia mediante el pago en línea por e-gold, que se utilizó para dirigir los fondos a través de varios países antes de llegar a su destino. El dinero blanqueado se usaba para financiar tanto el registro por parte de Tsouli de 180 sitios web que hospedaban videos de propaganda de Al-Qaida como el suministro de equipo para actividades terroristas en varios países. Se usaron unas 1.400 tarjetas de crédito para generar aproximadamente 1,6 millones de libras esterlinas de fondos ilícitos para financiar actividades terroristas¹².

16. El apoyo financiero a organizaciones aparentemente legítimas, tales como las organizaciones benéficas, también puede desviarse hacia fines ilícitos. Se sabe de algunas organizaciones terroristas que han establecido empresas fantasmas, disfrazadas de entidades filantrópicas, para solicitar donaciones en línea. Estas organizaciones pueden afirmar que apoyan causas humanitarias, cuando, en realidad, utilizan las donaciones para financiar actos de terrorismo. Entre las organizaciones aparentemente benéficas que se emplean con fines terroristas cabe mencionar la Benevolence International Foundation, la Global Relief Foundation y la Holy Land Foundation for Relief and Development, todas las cuales, pese a sus nombres inocuos, utilizan medios fraudulentos para financiar organizaciones terroristas en el Oriente Medio. Los terroristas también pueden infiltrarse en filiales de organizaciones de beneficencia, que utilizan como tapadera para promover las ideologías de organizaciones terroristas o para prestar apoyo material a grupos militantes¹³.

3. Adiestramiento

17. En los últimos años, las organizaciones terroristas han recurrido cada vez más a Internet como campamento de adiestramiento alternativo de terroristas. Hay una gama cada vez mayor de medios de comunicación que proporcionan plataformas para la difusión de guías prácticas en forma de manuales en línea, ficheros de audio y video, materiales de información y asesoramiento. Estas plataformas de Internet también ofrecen instrucciones detalladas, a menudo en formato multimedia de fácil acceso y en varios idiomas, sobre temas tales como la forma de afiliarse a organizaciones terroristas, cómo fabricar explosivos, armas de fuego u otras armas o materiales peligrosos, y cómo planear y ejecutar ataques terroristas. Las plataformas actúan a manera de campamentos de entrenamiento virtuales. También se utilizan para compartir, entre otras cosas, métodos, técnicas o conocimientos operacionales específicos con el fin de cometer actos de terrorismo.

18. Por ejemplo, *Inspire* es una revista en línea supuestamente publicada por Al-Qaida en la Península Arábiga con el objetivo declarado de permitir a los musulmanes entrenarse para la yihad en su casa. Contiene una gran cantidad de material ideológico destinado a fomentar el terrorismo, incluidas algunas declaraciones atribuidas a Osama Bin Laden, el jeque Ayman al-Zawahiri y otros conocidos cabecillas de

¹²Comunicación escrita del experto del Reino Unido.

¹³Maura Conway, "Terrorist 'use' of the Internet and fighting back", *Information & Security*, vol. 19 (2006), págs. 12 a 14.

Al-Qaida. La edición de otoño de 2010 contenía material didáctico práctico sobre cómo adaptar un vehículo de tracción en las cuatro ruedas para llevar a cabo un ataque contra miembros del público y cómo una sola persona podía lanzar un ataque indiscriminado disparando un arma de fuego desde una torre. La publicación sugería incluso una ciudad como blanco para dicho ataque, con el fin de aumentar las probabilidades de matar a un miembro del Gobierno¹⁴.

19. Los materiales de instrucción disponibles en línea incluyen herramientas para facilitar las actividades de contrainteligencia y piratería, así como para aumentar la seguridad de las comunicaciones y las actividades en línea ilícitas mediante el uso de las técnicas de cifrado y de anonimato existentes. El carácter interactivo de las plataformas de Internet ayuda a infundir un sentido de comunidad entre las personas de diferentes lugares geográficos y de distinto origen, lo cual fomenta la creación de redes para el intercambio de materiales de instrucción y tácticos.

4. Planificación

20. Muchos profesionales de la justicia penal han indicado que en casi todos los casos de terrorismo que se llevaron a juicio se había usado la tecnología de Internet. En particular, la planificación de un acto de terrorismo típicamente implica la comunicación a distancia entre varias partes. Un caso reciente de Francia, *Ministerio Público c. Hicheur*¹⁵, ilustra cómo se pueden utilizar diferentes formas de la tecnología de Internet para facilitar la preparación de actos de terrorismo, incluso mediante extensas comunicaciones dentro de una misma organización y entre organizaciones que promueven el extremismo violento, así como a través de las fronteras.

Ministerio Público c. Hicheur

En mayo de 2012, un tribunal francés condenó a Adlène Hicheur, nacional francés nacido en Argelia, a cinco años de prisión por su participación en una confabulación delictiva para la preparación de un acto terrorista (en virtud del artículo 421-1 y siguientes del Código Penal francés), en relación con actos que habían tenido lugar en Francia en 2008 y 2009.

La investigación de Hicheur, físico nuclear, se inició a principios de 2008 en relación con una comunicación electrónica de contenido yihadista, enviada al sitio web de la Presidencia de la República Francesa por un miembro, según se pudo comprobar, de Al-Qaida en el Magreb Islámico (AQMI).

Una orden de conservación dictada en enero de 2009 permitió a las autoridades descubrir un intercambio de mensajes electrónicos entre el miembro de AQMI y, entre otros, el Frente Mundial de Medios de Información Islámicos (GIMF) y el Centro Rafidayin, sitio web con el objetivo declarado de hospedar y difundir documentos, grabaciones de audio y video de

¹⁴Comunicación escrita del experto del Reino Unido.

¹⁵Sentencia de 4 de mayo de 2012, Causa núm. 0926639036 del Tribunal de Grande Instance de París (14a Cámara/2), París.

Al-Qaida, declaraciones de caudillos y atacantes suicidas y materiales de otros grupos extremistas islámicos. Los mensajes electrónicos intercambiados estaban cifrados mediante el software especializado "Asrar el Mojahedeen" o "Mujahedeen Secrets", que incluye cifrado de 256 bits, claves ocultas y variables de cifrado, claves de cifrado RSA de 2.048 bits y mensajería instantánea cifrada de foros de charla.

En el juicio se presentaron decenas de mensajes electrónicos cifrados. La fiscalía afirmó que el contenido de esos mensajes indicaba que Hicheur había llevado a cabo activamente, entre otros, los siguientes actos en apoyo de la red yihadista, en particular, en nombre del Centro Rafidayin:

- Tradujo, cifró, comprimió y protegió con contraseña materiales en favor de la yihad, incluidos documentos y videos, que luego cargó y distribuyó por Internet
- Distribuyó el software de cifrado "Mujahedeen Secrets" para facilitar las comunicaciones secretas por Internet
- Se confabuló con un miembro de AQMI para organizar y coordinar actividades yihadistas, que incluían, pero sin limitarse a ello, la prestación de apoyo financiero a la causa yihadista, la difusión de información en favor de la yihad y el apoyo a la creación de una unidad operacional en Europa y, en particular, en Francia, para preparar posibles atentados terroristas
- Se desempeñó como moderador en el sitio web yihadista Ribaat
- Tomó medidas concretas para proporcionar apoyo financiero a AQMI; entre otras, trató de usar PayPal y otros sistemas de pago virtuales.

En el juicio, la fiscalía afirmó que esas comunicaciones demostraban que Hicheur había sido plenamente consciente de que estaba en contacto con un miembro de AQMI, y que había actuado a sabiendas y voluntariamente como intermediario entre los combatientes yihadistas y el GIMF. Al concluir el juicio, el Tribunal declaró que: "Hicheur se convirtió ... en un apoyo logístico y de difusión de esta estructura terrorista para la cual 'la yihad en los medios de comunicación' es de importancia decisiva".

Además, el Tribunal sostuvo que "Adlène Hicheur, al prestar su acuerdo para la creación de una unidad operacional vinculada a AQMI en Europa, o incluso en Francia, y al seleccionar objetivos o categorías de objetivos para ser atacados, participó en un grupo [AQMI] creado específicamente para preparar actos de terrorismo".

El Tribunal concluyó, por tanto, que había pruebas suficientes para demostrar, según lo dispuesto en el Código Penal francés, que Hicheur había proporcionado no solo apoyo intelectual, sino también apoyo logístico directo a un plan claramente clasificado como terrorista. La decisión del tribunal es apelable.

Fuentes: Sentencia de 4 de mayo de 2012 del Tribunal de Grande Instance de París; y Tung, Liam, *Jihadists get world-class encryption kit* (29 de enero de 2008), disponible en www.zdnet.com.au/jihadists-get-world-class-encryption-kit-339285480.htm.

21. También se pueden tomar medidas a través de Internet para elegir el blanco potencial de un ataque y el medio más eficaz de lograr el propósito terrorista. Estas medidas preparatorias pueden ir, desde obtener instrucciones sobre los métodos recomendados de ataque, hasta la reunión de información de acceso público y de otra índole en relación con el blanco propuesto. La capacidad de Internet para salvar distancias y cruzar fronteras, y la gran cantidad de información a disposición del público

en el ciberespacio, hacen de Internet un instrumento ideal para la planificación de actos terroristas.

a) *Comunicaciones secretas preparatorias*

22. La función más básica de Internet es facilitar la comunicación. Los terroristas se han vuelto cada vez más expertos en la explotación de las tecnologías de las comunicaciones a fin de establecer contactos de manera anónima para la planificación de actos terroristas. Los terroristas pueden valerse de una simple cuenta de correo electrónico para comunicarse mediante contactos virtuales, a salvo de testigos, como si se tratara de un “buzón muerto”. Esto consiste en crear un borrador de mensaje, que no se envía, y deja, por tanto, rastros electrónicos mínimos, pero al que pueden acceder, mediante una conexión con Internet en cualquier parte del mundo, varias personas que sepan la contraseña necesaria.

23. Además, hay gran número de tecnologías más sofisticadas que aumentan la dificultad de identificar al remitente y al destinatario o conocer el contenido de las comunicaciones por Internet. Es fácil conseguir en línea instrumentos de cifrado y software de anonimato listos para ser descargados. Estos instrumentos pueden, entre otras cosas, enmascarar la dirección IP —el protocolo de Internet único que identifica cada dispositivo usado para acceder a Internet y su ubicación—, reencaminar las comunicaciones de Internet por uno o más servidores a jurisdicciones con niveles más bajos de represión de las actividades terroristas o cifrar los datos de tráfico relacionados con los sitios web visitados o ambas cosas. También se puede usar la esteganografía, el ocultamiento de mensajes en imágenes.

b) *Información de dominio público*

24. Las organizaciones y los particulares suelen publicar grandes cantidades de información en Internet. En el caso de las organizaciones, esto puede ser resultado, en parte, del deseo de promover sus actividades y optimizar su interacción con el público. También se puede conseguir información más confidencial, que pueden utilizar los terroristas con fines ilícitos, mediante los buscadores de Internet, que pueden catalogar y recuperar información insuficientemente protegida de millones de sitios web. Además, el acceso en línea a información logística detallada, como el acceso en tiempo real a imágenes de televisión de circuito cerrado, y aplicaciones como Google Earth, que están destinadas a ser utilizadas principalmente por particulares para fines legítimos, pueden ser usadas indebidamente por quienes intentan beneficiarse del libre acceso a las imágenes de satélite de alta resolución, mapas e información sobre terrenos y edificios para el reconocimiento de posibles objetivos desde una terminal de computadora remota.

25. Especialmente en la era de los populares medios de comunicación de las redes sociales como Facebook, Twitter, YouTube, Flickr y plataformas de blogs, muchas personas también publican por Internet, voluntaria o involuntariamente, una cantidad sin precedentes de información confidencial. Mientras que el propósito de quienes distribuyen la información puede ser proporcionar noticias o actualizaciones a su público con fines informativos o sociales, parte de esa información puede ser objeto de apropiación indebida y utilizada en provecho de actividades delictivas.

5. Ejecución

26. Algunos elementos de las categorías que se acaban de describir se pueden emplear en Internet para perpetrar actos terroristas. Por ejemplo, las amenazas explícitas de violencia, incluso en relación con el uso de armas, pueden difundirse por Internet para provocar ansiedad, miedo o pánico en una población o un sector de esta. En muchos Estados Miembros, el acto de difundir dichas amenazas, aunque no se cumplan, puede ser considerado un delito. Por ejemplo, en China, el acto de proferir una amenaza falsa y/o hacer circular una amenaza que se sabe que es falsa en relación con el uso de bombas o materiales biológicos, químicos o radiactivos u otras armas, cuando se comete con la intención de “perturbar gravemente el orden público”, está tipificado en la legislación nacional¹⁶. Las comunicaciones de Internet también pueden emplearse como medio para ponerse en contacto con las víctimas potenciales o para coordinar la ejecución de actos físicos de terrorismo. Por ejemplo, se hizo un amplio uso de Internet para coordinar las actividades de los participantes en los atentados del 11 de septiembre de 2001 en los Estados Unidos.

27. El uso de Internet para facilitar la ejecución de actos terroristas puede, entre otras cosas, ofrecer ventajas logísticas, reducir las probabilidades de detección y encubrir la identidad de los responsables. El acceso a Internet también puede facilitar la adquisición de los elementos necesarios para la ejecución del ataque. Los terroristas pueden adquirir cada uno de los componentes o servicios requeridos para perpetrar actos violentos de terrorismo mediante el comercio electrónico. La apropiación indebida de tarjetas de crédito u otras formas fraudulentas de pago electrónico pueden emplearse para financiar dichas compras.

6. Ciberataques

28. Un ciberataque generalmente se refiere a la explotación deliberada de redes informáticas como medio de lanzar un ataque. Estos ataques suelen estar destinados a perturbar el funcionamiento normal de los blancos elegidos, como los sistemas de computadoras, servidores o la infraestructura subyacente, mediante el uso de técnicas de piratería informática, amenazas avanzadas y persistentes, virus informáticos, programas maliciosos¹⁷, phlooding¹⁸ o cualquier otro medio de acceso no autorizado o malicioso. Los ciberataques pueden tener todas las características de un acto de terrorismo, incluido el deseo fundamental de infundir miedo en apoyo de objetivos políticos o sociales. Cabe citar, como ejemplo de ciberataque, el sufrido por Israel en enero de 2012, que consistió en ataques contra múltiples sitios web israelíes simbólicos, como los sitios web de la Bolsa de Valores de Tel Aviv y la compañía aérea nacional, así como

¹⁶Comunicación escrita del experto de China.

¹⁷Según el Manual de la Unión Internacional de Telecomunicaciones sobre legislación contra la ciberdelincuencia, sección 1 (n), los programas maliciosos o malignos pueden definirse como programas que se insertan en un programa o sistema de computadora, generalmente de manera encubierta, con la intención de comprometer la confidencialidad, integridad o disponibilidad de los programas, datos o sistemas de una computadora.

¹⁸“Phlooding” se refiere al ataque dirigido contra los servidores de autenticación centrales de una organización con múltiples solicitudes de autenticación simultáneas, con objeto de sobrecargar los servidores, lo cual ocasiona una denegación de servicio distribuida.

la divulgación no autorizada de los detalles de cuentas de tarjetas de crédito de miles de nacionales israelíes¹⁹. Si bien en los últimos años se ha prestado considerable atención a la amenaza de ciberataques por terroristas, este tema está más allá del alcance de la presente publicación y, por tanto, no será objeto de análisis.

C. Uso de Internet para combatir las actividades terroristas

29. Mientras que los terroristas han ideado muchas formas de valerse de Internet para fines ilícitos, el uso de Internet también ofrece oportunidades de reunir inteligencia y desarrollar otras actividades para prevenir y combatir los actos de terrorismo, así como de obtener pruebas para el enjuiciamiento de esos actos. De las comunicaciones de los sitios web, salas de charla y otras comunicaciones de Internet se puede extraer una cantidad importante de información sobre el funcionamiento, las actividades y, en ocasiones, los blancos de las organizaciones terroristas. Además, el uso cada vez mayor de Internet con fines terroristas proporciona un aumento concomitante de la disponibilidad de datos electrónicos que pueden reunirse y analizarse para combatir el terrorismo. Las fuerzas del orden, los servicios de inteligencia y otras autoridades están creando instrumentos cada vez más sofisticados para detectar, prevenir o disuadir, de manera proactiva, las actividades terroristas que se sirven de Internet. También se está expandiendo la utilización de los medios de investigación tradicionales, como los servicios de traducción especializados para la detección oportuna de posibles amenazas terroristas.

30. Las discusiones en línea ofrecen la oportunidad de presentar puntos de vista opuestos o participar en debates constructivos, que pueden tener el efecto de desalentar a posibles partidarios. Los contraargumentos con una base fáctica sólida pueden exponerse en foros de debate en línea, con imágenes y videos. El éxito de los mensajes también puede depender de que manifiesten empatía por los problemas subyacentes que contribuyen a la radicalización, como las condiciones políticas y sociales, y presenten alternativas a los medios violentos para lograr los resultados deseados²⁰. Las comunicaciones estratégicas que ofrecen contraargumentos a la propaganda terrorista también pueden difundirse a través de Internet, en varios idiomas, para llegar a un público amplio y geográficamente diverso.

31. El Centro de Comunicaciones Estratégicas contra el Terrorismo, con sede en los Estados Unidos, ofrece un ejemplo de una iniciativa interinstitucional lanzada recientemente que tiene por objeto reducir la radicalización y la violencia extremista mediante

¹⁹Véase Isabel Kershner, “Cyberattack exposes 20,000 Israeli credit card numbers and details about users”, *New York Times*, 6 de enero de 2012, y “2 Israeli web sites crippled as cyberwar escalates”, *New York Times*, 16 de enero de 2012.

²⁰Equipo Especial sobre la Ejecución de la Lucha contra el Terrorismo, del Grupo de Trabajo sobre medidas para hacer frente al uso de Internet con fines terroristas, “Conference summary and follow-up/recommendations” de la Conferencia sobre la utilización de Internet para contrarrestar la atracción de la violencia extremista, celebrada en Riad del 24 al 26 de enero de 2011. Puede consultarse en www.un.org/en/terrorism/ctitf/pdfs/ctitf_riyadh_conference_summary_recommendations.pdf.

la detección a tiempo de propaganda extremista, entre otras cosas, en Internet, y responder rápidamente con contraargumentos dirigidos mediante una amplia gama de tecnologías de las comunicaciones, incluidas las herramientas digitales²¹. Por ejemplo, según se informó, en mayo de 2012 el Centro respondió, dentro de las 48 horas, a anuncios publicitarios que promovían la violencia extremista aparecidos en varios sitios web de Al-Qaida en la Península Arábiga, con contraargumentos publicados en esos mismos sitios web que presentaban una versión modificada de ese mismo mensaje con el fin de demostrar que las víctimas de las actividades de la organización terrorista eran ciudadanos yemeníes. La campaña de contraargumentos fue posible gracias a la cooperación entre el Departamento de Estado de los Estados Unidos, la comunidad de los servicios de inteligencia y las autoridades militares. El Centro también utiliza plataformas de redes sociales como Facebook y YouTube para sus comunicaciones con contraargumentos^{22,23}.

D. Consideraciones fundadas en el estado de derecho

32. El respeto por los derechos humanos y el estado de derecho es parte integrante de la lucha contra el terrorismo. Debe ponerse especial cuidado en respetar las normas internacionales de derechos humanos en todas las fases de las iniciativas de lucha contra el terrorismo, desde la reunión de inteligencia con fines preventivos hasta el enjuiciamiento de los sospechosos, en que deben respetarse las garantías procesales. Esto exige el desarrollo de leyes y prácticas nacionales de lucha contra el terrorismo que promuevan y protejan los derechos humanos fundamentales y el estado de derecho²⁴.

33. Los Estados tienen el derecho y el deber de adoptar medidas eficaces para contrarrestar el impacto destructivo del terrorismo en los derechos humanos, en particular los derechos a la vida, a la libertad y a la integridad física de las personas y la integridad territorial y la seguridad de los Estados. Las medidas eficaces contra el terrorismo y la protección de los derechos humanos son objetivos complementarios que se refuerzan mutuamente y deben perseguirse al mismo tiempo²⁵. Las iniciativas de lucha contra el terrorismo relacionadas con el uso de Internet pueden influir en el disfrute de una serie de derechos humanos, incluidos los derechos a la libertad de expresión, la libertad de asociación, la privacidad y juicios imparciales. Si bien un análisis exhaustivo de las cuestiones de derechos humanos está más allá del alcance de la presente publicación, es importante poner de relieve ciertas esferas clave que conviene considerar.

²¹Orden Ejecutiva 13584, de 9 de septiembre de 2011, "Developing an Integrated Strategic Counterterrorism Communications Initiative and Establishing a Temporary Organization to Support Certain Government-wide Communications Activities Directed Abroad", *Federal Register*, vol. 76, núm. 179, 15 de septiembre de 2011.

²²"United States State Department fights al-Qaeda in cyberspace", *Al Jazeera* (25 de mayo de 2012). Puede consultarse en <http://blogs.aljazeera.com/americas/2012/05/25/us-state-department-fights-al-qaeda-cyberspace>.

²³"U.S. uses Yemeni web sites to counter al-Qaeda propaganda", *The Washington Post* (24 de mayo de 2012). Puede consultarse en www.washingtonpost.com/world/national-security/us-hacks-web-sites-of-al-qaeda-affiliate-in-yemen/2012/05/23/gJQAGnOxIU_story.html.

²⁴Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, Folleto informativo núm. 32, cap. III, secc. H.

²⁵*Ibid.*, cap. I, secc. C.

34. Como se señaló en la subsección B. 1 *b) supra*, la prohibición de la incitación al terrorismo puede implicar restricciones a la libertad de expresión. La libertad de expresión no es un derecho absoluto. Se puede restringir, a condición de que la restricción satisfaga pruebas estrictamente concebidas de legalidad, necesidad, proporcionalidad y no discriminación, cuando esa libertad se usa para incitar a la discriminación, la hostilidad o la violencia. Una de las principales dificultades en los casos de glorificación del terrorismo o de incitación a cometer actos terroristas es determinar por dónde pasa la línea de aceptabilidad, ya que esto varía mucho de un país a otro, según las diferentes historias culturales y jurídicas²⁶. El derecho a la libertad de asociación es igualmente un derecho limitado, que puede ser objeto de restricciones y excepciones de interpretación estricta.

35. La lucha contra el uso terrorista de Internet puede implicar la vigilancia de sospechosos y la reunión de información sobre ellos. Debe prestarse especial atención a la protección de las personas contra las injerencias arbitrarias o ilegales en su derecho a la vida privada²⁷, que incluye el derecho al carácter confidencial de la información sobre la identidad de una persona, así como su vida privada. Las leyes nacionales deben ser suficientemente detalladas con respecto, entre otras cosas, a las circunstancias específicas en que puede permitirse tal injerencia. Deben existir garantías apropiadas para evitar el abuso de los instrumentos de vigilancia secreta. Además, todos los datos personales recogidos deberán estar debidamente protegidos para defenderse contra el acceso, la divulgación o el uso ilegales o arbitrarios²⁸.

36. Velar por las garantías procesales es fundamental para asegurarse de que las medidas antiterroristas sean eficaces y respeten el estado de derecho. La protección de los derechos humanos de todas las personas acusadas de delitos penales, incluidos los relacionados con el terrorismo, abarca el derecho a la presunción de inocencia, el derecho a un juicio con las debidas garantías y dentro de un plazo razonable, por un tribunal competente, independiente e imparcial y el derecho a que la condena y la sentencia puedan ser revisadas por un tribunal superior que cumpla las mismas normas²⁹.

37. Para un análisis más detallado de las cuestiones destacadas en la presente sección y otras consideraciones pertinentes, véase, por ejemplo, el Folleto informativo núm. 32 de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos sobre “Los derechos humanos, el terrorismo y la lucha contra el terrorismo”, el informe de la Alta Comisionada de las Naciones Unidas para los Derechos Humanos sobre la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo (A/HRC/16/50) y los siguientes informes del Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en

²⁶Organización para la Seguridad y la Cooperación en Europa, Oficina de Instituciones Democráticas y Derechos Humanos, “Human rights considerations in combating incitement to terrorism and related offences”, documento de antecedentes preparado para la Reunión de expertos sobre la prevención del terrorismo: la lucha contra la incitación al terrorismo y contra las actividades terroristas conexas, celebrada en Viena los días 19 y 20 de octubre de 2006, secciones 3 y 4.

²⁷Véase el Pacto Internacional de Derechos Civiles y Políticos, art. 17.

²⁸“Los derechos humanos, el terrorismo y la lucha contra el terrorismo”, cap. III, secc. J.

²⁹Ibid., cap. III, secc. F.

la lucha contra el terrorismo: Diez esferas de mejores prácticas en la lucha contra el terrorismo (A/HRC/16/51), y Recopilación de buenas prácticas relacionadas con los marcos y las medidas de carácter jurídico e institucional que permitan garantizar el respeto de los derechos humanos por los servicios de inteligencia en la lucha contra el terrorismo, particularmente en lo que respecta a su supervisión (A/HRC/14/46).

II. El contexto internacional

A. Introducción

38. El uso de Internet por los terroristas es un problema transnacional que requiere una respuesta integrada a través de las fronteras y entre los distintos sistemas nacionales de justicia penal. Las Naciones Unidas desempeñan un papel fundamental en este sentido, facilitando el debate y el intercambio de buenas prácticas entre los Estados Miembros, y ayudando a crear un consenso sobre enfoques comunes para combatir el uso de Internet con fines terroristas.

39. El marco jurídico internacional aplicable en relación con la lucha contra el terrorismo se encuentra en una variedad de fuentes, entre otras, las resoluciones de la Asamblea General y el Consejo de Seguridad, los tratados, la doctrina legal y el derecho internacional consuetudinario. Las resoluciones del Consejo de Seguridad pueden imponer obligaciones jurídicamente vinculantes para los Estados Miembros o proporcionar fuentes de compromisos políticos de “derecho incipiente” o normas nacientes de derecho internacional. Las resoluciones del Consejo aprobadas en virtud del Capítulo VII de la Carta de las Naciones Unidas son vinculantes para todos los Estados Miembros. La Asamblea General también ha aprobado una serie de resoluciones sobre terrorismo que proporcionan fuentes útiles de derecho incipiente y tienen gran importancia política, a pesar de no ser jurídicamente vinculantes³⁰.

40. Los Estados también contraen obligaciones jurídicas en virtud de los instrumentos bilaterales y multilaterales que tratan del terrorismo. Son instrumentos jurídicos “universales” los acuerdos que están abiertos a la ratificación o adhesión de todos los Estados Miembros de las Naciones Unidas. Los acuerdos concertados por agrupaciones regionales o interestatales, en cambio, pueden estar abiertos solo a un grupo limitado de signatarios potenciales; las obligaciones dimanadas de esos tratados son vinculantes únicamente para aquellos Estados que deciden ser partes en los acuerdos.

41. El deber de enjuiciar a los autores de actos terroristas recae principalmente en las autoridades nacionales, pues los tribunales internacionales por lo general no son competentes para entender en tales causas³¹. Las resoluciones de las Naciones Unidas, los instrumentos jurídicos universales, los acuerdos regionales y las leyes modelo contra

³⁰Véase Oficina de las Naciones Unidas contra la Droga y el Delito, Preguntas frecuentes sobre cuestiones de derecho internacional de la lucha contra el terrorismo (2009). Puede consultarse en <http://www.unodc.org/documents/terrorism/Publications/FAQ/Spanish.pdf>.

³¹El Tribunal Especial para el Líbano, establecido en virtud de la resolución 1757 (2007) del Consejo de Seguridad, es actualmente el único tribunal internacional con competencia limitada sobre el delito de terrorismo.

el terrorismo desempeñan un papel clave en el establecimiento de normas comunes aceptadas en múltiples ordenamientos jurídicos.

B. Resoluciones de las Naciones Unidas contra el terrorismo

42. La Asamblea General aprobó por unanimidad la Estrategia global contra el terrorismo³² en 2006, lo que representa un hito en el ámbito de las iniciativas multilaterales de lucha contra el terrorismo. De conformidad con la Estrategia, los Estados Miembros resolvieron, entre otras cosas:

- a) Condenar, de manera sistemática, inequívoca y firme, el terrorismo en todas sus formas y manifestaciones, independientemente de quién lo cometa y de dónde y con qué propósitos, puesto que constituye una de las amenazas más graves para la paz y la seguridad internacionales;
- b) Adoptar medidas urgentes para prevenir y combatir el terrorismo en todas sus formas y manifestaciones;
- c) Reconocer que la cooperación internacional y todas las medidas que [ellos] adopten para prevenir y combatir el terrorismo deben ajustarse a las obligaciones que les incumben en virtud del derecho internacional, incluida la Carta de las Naciones Unidas y los convenios y protocolos internacionales pertinentes, en particular las normas de derechos humanos, el derecho de los refugiados y el derecho internacional humanitario;
- d) Cooperar con las Naciones Unidas, teniendo debidamente en cuenta la confidencialidad, respetando los derechos humanos y de conformidad con otras obligaciones dimanadas del derecho internacional, a fin de estudiar formas de “a) *Coordinar esfuerzos, a nivel regional e internacional, para luchar contra el terrorismo en todas sus formas y manifestaciones en Internet; b) Utilizar Internet como instrumento para luchar contra la propagación del terrorismo, reconociendo al mismo tiempo que los Estados pueden necesitar asistencia a este respecto*” [sin cursiva en el original].

43. Varias resoluciones del Consejo de Seguridad aprobadas en los últimos años obligan a los Estados a cooperar sin reservas en la lucha contra el terrorismo, en todas sus formas. En particular, las resoluciones 1373 (2001) y 1566 (2004), aprobadas en virtud del Capítulo VII de la Carta de las Naciones Unidas, requieren que todos los Estados Miembros adopten medidas legislativas y de otro tipo para luchar contra el terrorismo, incluso mediante una mayor cooperación con otros gobiernos en la investigación, detección, detención, extradición y enjuiciamiento de los implicados en actos terroristas, y exhortan a los Estados a aplicar los convenios y protocolos internacionales relativos al terrorismo.

44. Otra resolución clave del Consejo de Seguridad relativa a la actividad terrorista que puede llevarse a cabo por medio de Internet es la resolución 1624 (2005), que aborda la incitación y la glorificación de actos terroristas. En el párrafo cuarto del preámbulo, el Consejo condena “la incitación a la comisión de actos de terrorismo” y repudia “los intentos de justificación o glorificación (apología) de actos de terrorismo que puedan incitar a la comisión de nuevos actos de terrorismo”. En el párrafo 1 se insta a todos los Estados a que adopten las medidas necesarias y adecuadas en cumplimiento de sus obligaciones de derecho internacional para prohibir por ley la incitación a la comisión de un acto o actos de terrorismo.

45. En recientes informes y resoluciones de las Naciones Unidas se ha reconocido expresamente la importancia de la lucha contra el uso terrorista de Internet como elemento clave de una amplia estrategia contra el terrorismo. En su informe de 2006 a la Asamblea General titulado “Unidos contra el terrorismo: recomendaciones para una estrategia mundial de lucha contra el terrorismo”³³, el Secretario General declaró de manera explícita: “La capacidad para generar y transferir fondos, adquirir armas, captar y adiestrar nuevos miembros y comunicarse, especialmente mediante el uso de Internet, resulta esencial para los terroristas”³⁴. El Secretario General continuó diciendo que la importancia de Internet como vehículo de proselitismo, información y propaganda por parte de los terroristas aumentaba rápidamente, lo cual debía ser contrarrestado mediante la acción coordinada de los Estados Miembros, respetando los derechos humanos y en consonancia con las obligaciones contraídas en virtud del derecho internacional³⁵.

46. En su resolución 1963 (2010), el Consejo de Seguridad expresó “su preocupación ante la creciente utilización por los terroristas, en una sociedad globalizada, de nuevas tecnologías de la información y las comunicaciones, en particular Internet, con fines de reclutamiento e incitación, así como para financiar, planificar y preparar sus actividades”. El Consejo también reconoció la importancia de que los Estados Miembros actuaran en cooperación para impedir que los terroristas aprovecharan las tecnologías, las comunicaciones y los recursos de Internet.

C. Instrumentos jurídicos universales contra el terrorismo

47. Desde 1963, la comunidad internacional ha venido elaborando instrumentos jurídicos universales para prevenir los actos de terrorismo bajo los auspicios de las Naciones Unidas y sus organismos especializados, en particular la Organización de Aviación Civil Internacional, la Organización Marítima Internacional y el Organismo Internacional de Energía Atómica. Los instrumentos universales contra el terrorismo representan un elemento central del régimen mundial contra el terrorismo y un marco importante para la cooperación internacional contra el terrorismo. Estos instrumentos jurídicos universales abarcan actos que van desde el secuestro de aviones hasta el terrorismo nuclear

³³A/60/825.

³⁴Ibid., párr. 38.

³⁵Ibid., párrs. 58 y 60.

por parte de personas y grupos³⁶ y obligan a los Estados que los ratifiquen a penalizar los actos terroristas más previsibles en los ámbitos cubiertos por los convenios. Sin embargo, estos instrumentos jurídicos universales son jurídicamente vinculantes únicamente para sus firmantes³⁷, que también son responsables de hacer cumplir las disposiciones mediante sus sistemas nacionales de justicia penal.

48. Como resultado de la atención prestada a la lucha contra el terrorismo a raíz de la aprobación de la resolución 1373 (2001) del Consejo de Seguridad, en que el Consejo instaba a los Estados Miembros a que se adhiriesen a los instrumentos jurídicos universales contra el terrorismo, el ritmo de adhesión a esos instrumentos aumentó apreciablemente. En junio de 2011, dos tercios de los Estados Miembros habían ratificado o se habían adherido a por lo menos 10 de los 16 instrumentos universales contra el terrorismo³⁸.

49. Actualmente no hay ningún tratado amplio de las Naciones Unidas contra el terrorismo que sea aplicable a una lista exhaustiva de las manifestaciones de terrorismo. Del mismo modo, la comunidad internacional todavía no se ha puesto de acuerdo sobre una definición internacional jurídicamente vinculante del término “terrorismo”³⁹, debido en gran parte a la dificultad de elaborar una categorización jurídica universalmente aceptable de los actos de violencia cometidos por los Estados, por grupos armados, como los movimientos de liberación o de libre determinación, o por particulares.

50. Los Estados Miembros vienen participando desde el año 2000 en las negociaciones relativas a una amplia convención contra el terrorismo, que contendrá, en definitiva, una definición del terrorismo. Sin embargo, frente a la dificultad de alcanzar un consenso sobre una definición única y aceptada en todo el mundo de lo que constituye terrorismo, se han hecho progresos, en cambio, a través de los actuales instrumentos jurídicos universales, que se han desarrollado a lo largo de líneas sectoriales. Estos instrumentos se centran en la penalización de determinados “actos terroristas”, sin definir el concepto más amplio de terrorismo.

51. Los instrumentos universales no definen los delitos terroristas como delitos con arreglo al derecho internacional. Más bien, se establece la obligación para los Estados partes en los acuerdos de penalizar en su derecho interno la conducta ilícita especificada, ejercer la competencia respecto de los autores en ciertas condiciones previstas y establecer mecanismos de cooperación internacional que permitan a los Estados partes

³⁶Entre otros actos de terrorismo incluidos, cabe mencionar los siguientes: actos de sabotaje contra la aviación, actos de violencia en los aeropuertos, actos contra la seguridad de la navegación marítima, actos contra la seguridad de las plataformas fijas emplazadas en la plataforma continental, delitos contra personas internacionalmente protegidas (como el secuestro de diplomáticos), actos ilícitos de apoderamiento y posesión de material nuclear, actos de toma de rehenes, atentados terroristas cometidos con bombas, financiación para la comisión de actos terroristas y organizaciones terroristas.

³⁷La lista del estado actual de ratificación de estos instrumentos jurídicos universales puede consultarse en https://www.unodc.org/tldb/es/universal_instruments_NEW.html?

³⁸Véase <http://www.un.org/es/sc/ctc/laws.html>.

³⁹Vale la pena señalar, sin embargo, que una reciente decisión del Tribunal Especial para el Líbano sostuvo que había pruebas suficientes para apoyar la existencia de una definición del delito de terrorismo en el derecho internacional consuetudinario. Véase Interlocutory Decision on the Applicable Law: Terrorism, Conspiracy, Homicide, Perpetration, Cumulative Charging, Case núm. STL-11-01/I, Tribunal Especial para el Líbano (16 de febrero de 2011); puede consultarse en www.stl-tsl.org/en/the-cases/stl-11-01/rule-176bis/filings/orders-and-decisions/appeals-chamber/f0010.

enjuiciar o extraditar a los presuntos autores. Mientras no se concluyan con éxito las negociaciones en curso sobre una definición universal o convenio general sobre el terrorismo, los acuerdos bilaterales y multilaterales deberán servir de base para la elaboración de normas comunes para combatir el uso de Internet con fines terroristas, en aras de la promoción de la cooperación internacional.

52. No existe ningún convenio universal que trate específicamente de la prevención y represión del uso de Internet por terroristas. En diciembre de 2010, la Asamblea General aprobó la resolución 65/230, en la que, entre otras cosas, hizo suya la Declaración de Salvador sobre estrategias amplias ante problemas globales: los sistemas de prevención del delito y justicia penal y su desarrollo en un mundo en evolución⁴⁰ y solicitó a la Comisión de Prevención del Delito y Justicia Penal que estableciera, con arreglo a lo dispuesto en la Declaración de Salvador, un grupo intergubernamental de expertos de composición abierta para que realizara un estudio exhaustivo del problema del delito cibernético y de las respuestas de los Estados Miembros, la comunidad internacional y el sector privado ante ese fenómeno, incluido el intercambio de información sobre legislación nacional, mejores prácticas, asistencia técnica y cooperación internacional. Los resultados de este estudio, lanzado por la UNODC en febrero de 2012, facilitarán la evaluación de los efectos del uso de las nuevas tecnologías de la información en apoyo de actividades delictivas, en particular con respecto a ciertos usos terroristas de Internet, tales como la incitación al terrorismo y a la comisión de delitos de financiación del terrorismo por medios informáticos.

D. Normas jurídicas internacionales de derechos humanos

53. Las obligaciones en materia de derechos humanos constituyen parte integrante del marco jurídico internacional de lucha contra el terrorismo y se traducen en la obligación impuesta a los Estados de prevenir los atentados terroristas, que pueden socavar considerablemente los derechos humanos, y en la obligación de velar por que en toda actividad de lucha contra el terrorismo se respeten los derechos humanos. En la Estrategia global de las Naciones Unidas contra el terrorismo, los Estados Miembros reafirmaron esas obligaciones, reconociendo en particular que “las medidas eficaces contra el terrorismo y la protección de los derechos humanos no son objetivos contrapuestos, sino que se complementan y refuerzan mutuamente”.

54. Entre los principales instrumentos universales de derechos humanos aprobados bajo los auspicios de las Naciones Unidas cabe mencionar la Declaración Universal de Derechos Humanos⁴¹, el Pacto Internacional de Derechos Civiles y Políticos y el Pacto Internacional de Derechos Económicos, Sociales y Culturales⁴², así como los protocolos aplicables.

⁴⁰Aprobada por el 12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, celebrado en Salvador (Brasil) del 12 al 19 de abril de 2010, que trata, entre otras cosas, de la necesidad de que los Estados Miembros consideren la manera de combatir las nuevas formas de delincuencia, como el delito cibernético.

⁴¹Resolución de la Asamblea General 217 A (III).

⁴²Resolución de la Asamblea General 2200 A (XXI), anexo.

55. Varias organizaciones regionales también han elaborado convenios que garantizan los derechos humanos. Entre otros, cabe mencionar el Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales⁴³ (1950), la Convención Americana sobre Derechos Humanos⁴⁴ (1969), la Carta africana de derechos humanos y de los pueblos⁴⁵ (1981), y la Carta de los derechos fundamentales de la Unión Europea (2000)⁴⁶.

56. Si bien un análisis exhaustivo de las cuestiones relativas a los derechos humanos está más allá del alcance de la presente publicación, se considerarán las cuestiones del estado de derecho y los instrumentos jurídicos aplicables en relación con medidas concretas contra el terrorismo cuando el contexto así lo aconseje⁴⁷.

E. Instrumentos jurídicos regionales y subregionales contra el terrorismo

57. Además de los instrumentos universales contra el terrorismo, hay varios instrumentos regionales y subregionales que ofrecen valiosas normas de fondo y de procedimiento para penalizar los actos de terrorismo que pueden ser perpetrados por medio de Internet. Estos instrumentos, que complementan los instrumentos universales contra el terrorismo, pueden variar en su alcance y en su grado de aplicabilidad.

I. Consejo de Europa

58. En 2001, el Consejo de Europa elaboró el Convenio sobre el delito cibernético⁴⁸, que es actualmente el único instrumento multilateral jurídicamente vinculante que trata de la actividad delictiva realizada en Internet. El Convenio sobre el delito cibernético del Consejo de Europa tiene por objeto armonizar las legislaciones nacionales relativas al delito cibernético, mejorar los procedimientos internos para detectar, investigar y perseguir esos delitos y proporcionar arreglos de cooperación internacional rápida y fiable sobre estas cuestiones⁴⁹. El Convenio establece una norma mínima común respecto de los delitos internos cometidos con computadoras⁵⁰ y prevé la penalización de nueve delitos, incluidos los delitos relacionados con el acceso no autorizado a sistemas, programas o datos informáticos, y la manipulación ilícita de estos; el fraude y la falsificación informáticos, y la tentativa de cometer tales actos o complicidad en su comisión⁵¹.

⁴³Consejo de Europa, *European Treaty Series*, núm. 5.

⁴⁴Naciones Unidas, *Treaty Series*, vol. 1144, núm. 17955.

⁴⁵Ibid., vol. 1520, núm. 26363.

⁴⁶*Diario Oficial de las Comunidades Europeas*, C 364, 18 de diciembre de 2000.

⁴⁷Véase también Oficina de las Naciones Unidas contra la Droga y el Delito, Preguntas frecuentes sobre cuestiones de derecho internacional de la lucha contra el terrorismo, secc. V.

⁴⁸Consejo de Europa, *European Treaty Series*, núm. 185 (también puede consultarse en www.coe.int/cybercrime).

⁴⁹Ibid., preámbulo.

⁵⁰Informe explicativo del Convenio sobre el delito cibernético del Consejo de Europa, párr. 33. Puede consultarse en http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS%20185%20Explanatory%20report_Spanish.pdf.

⁵¹Ibid., arts. 2 a 8 y 11.

59. El Convenio sobre el delito cibernético del Consejo de Europa también contiene importantes disposiciones de procedimiento que pueden facilitar la investigación y obtención de pruebas en relación con actos de terrorismo cometidos por Internet. Estas disposiciones son aplicables a cualquier delito cometido por medio de una computadora y a la reunión de pruebas electrónicas, y están sujetas a las garantías aplicables establecidas en la legislación nacional⁵².

60. Por ejemplo, el Convenio sobre el delito cibernético del Consejo de Europa obliga a las partes a promulgar leyes que exijan a los proveedores de servicios de Internet conservar los datos especificados almacenados en sus servidores durante un plazo máximo de 90 días⁵³ (renovable), si así se lo solicitan los funcionarios encargados de hacer cumplir la ley en el curso de una investigación o procedimiento penal, hasta que se puedan adoptar las medidas jurídicas apropiadas para exigir la divulgación de esos datos⁵⁴. Este procedimiento acelerado para la conservación de los datos almacenados tiene una importancia crítica dado el carácter efímero de los datos electrónicos y el largo tiempo que suelen llevar los procedimientos tradicionales de asistencia judicial recíproca en casos transnacionales⁵⁵. La emisión de una orden de conservación, o una medida similar, también tiene varias ventajas en comparación con los procedimientos tradicionales de registro e incautación, ya que el proveedor de servicios de Internet puede estar en mejores condiciones de obtener rápidamente las pruebas de que se trata. Además, una medida de conservación puede ser menos perjudicial para las operaciones legítimas del proveedor de servicios de Internet, con menos probabilidades de un posible perjuicio para la reputación de la empresa⁵⁶, lo cual facilita, a su vez, la cooperación establecida. El registro y la incautación de los datos almacenados, previstos en el artículo 19 del Convenio sobre el delito cibernético del Consejo de Europa, confiere a los datos almacenados una protección similar a la que suele otorgarse a las pruebas tangibles⁵⁷ de acuerdo con la legislación nacional pertinente⁵⁸.

61. El Convenio sobre el delito cibernético del Consejo de Europa también obliga a las partes a aplicar la legislación relativa a la presentación de los datos almacenados sobre los abonados⁵⁹. Dicha información puede ser de importancia decisiva en la etapa de investigación para establecer la identidad del autor de un acto terrorista que

⁵²Ibid., art. 14, párr. 2 b) y c), y art. 15. Dichas garantías incluyen la protección de los derechos humanos y las libertades, incluidos los derechos derivados de las obligaciones contraídas en virtud del Convenio para la Protección de los Derechos Humanos y las Libertades Fundamentales, el Pacto Internacional de Derechos Civiles y Políticos, otros instrumentos internacionales de derechos humanos, y decisiones judiciales u otra forma de supervisión independiente.

⁵³Se impone un mínimo de 60 días con respecto a la conservación ordenada en respuesta a una solicitud de asistencia judicial recíproca (Convenio sobre el delito cibernético del Consejo de Europa, art. 29).

⁵⁴Convenio sobre el delito cibernético del Consejo de Europa, art. 16.

⁵⁵Informe explicativo del Convenio sobre el delito cibernético del Consejo de Europa, párr. 157.

⁵⁶Ibid., párr. 155.

⁵⁷Como el medio físico, por ejemplo, en que se almacenan los datos.

⁵⁸Informe explicativo del Convenio sobre el delito cibernético del Consejo de Europa, párr. 184.

⁵⁹Véase Convenio sobre el delito cibernético del Consejo de Europa, art. 18. Por “datos relativos a los abonados” se entenderá cualquier información, diferente de los datos relativos al tráfico o al contenido, que se refiera a la identidad, la dirección postal o situación geográfica del abonado, número de teléfono o cualquier otro número de acceso, y los datos relativos a la facturación y al pago o cualquier otra información relativa al lugar en que se encuentren los equipos de comunicación, disponible en virtud de un contrato o de un acuerdo de prestación de servicio con el proveedor de los servicios de Internet.

involucre el uso de Internet, y puede incluir la ubicación física de esa persona, así como datos sobre otros servicios de comunicación conexos empleados en la comisión del hecho. El Convenio también obliga a los Estados signatarios a establecer normas mínimas para permitir la obtención en tiempo real de los datos de tráfico⁶⁰ asociados a comunicaciones específicas y la interceptación de datos de contenido en relación con determinados delitos graves conforme al derecho interno⁶¹.

62. El Convenio sobre el delito cibernético del Consejo de Europa puede aplicarse en conjunción con instrumentos de lucha contra el terrorismo, tales como el Convenio Europeo para la Prevención del Terrorismo⁶², a fin de proporcionar una base jurídica para la cooperación contra el uso de Internet con fines terroristas. El Convenio Europeo para la Prevención del Terrorismo obliga a las partes a tipificar como delitos ciertos actos de jurisdicción interna, que pueden dar lugar a la comisión de delitos de terrorismo, como la incitación pública, el reclutamiento y adiestramiento, todo lo cual puede hacerse por Internet. El Convenio también prescribe la adopción de medidas de cooperación nacional e internacional destinadas a prevenir el terrorismo, incluidas las medidas de investigación. Por ejemplo, el artículo 22 del Convenio prevé el intercambio con otras partes de información no solicitada en relación con investigaciones o actuaciones, dentro de los límites impuestos por la legislación nacional, en el interés común de responder a los actos delictivos (información espontánea).

63. El Convenio sobre el delito cibernético del Consejo de Europa y el Convenio Europeo para la Prevención del Terrorismo están abiertos a la ratificación o adhesión de todos los Estados miembros del Consejo de Europa⁶³, los Estados no miembros que participaron en la elaboración de esos convenios y otros Estados no miembros que fueron invitados, con el acuerdo de todos los Estados que entonces eran Partes en el Convenio pertinente⁶⁴. Cabe señalar que varios países que no se han adherido oficialmente al Convenio sobre el delito cibernético han utilizado sus disposiciones, no obstante, como directrices en la elaboración de su propia legislación nacional para reprimir la ciberdelincuencia. (Véase también la sección F, *infra*, sobre la legislación modelo.)

64. El Consejo de Europa elaboró también el Protocolo adicional al Convenio sobre el delito cibernético relativo a la penalización de actos de índole racista y xenófoba

⁶⁰Según el artículo 1 *d*) del Convenio sobre el delito cibernético del Consejo de Europa, los “datos relativos al tráfico” incluyen la información que indica el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente.

⁶¹De conformidad con los artículos 20 y 21, respectivamente, del Convenio sobre el delito cibernético.

⁶²Consejo de Europa, *Treaty Series*, núm. 196. También puede consultarse en <http://conventions.coe.int/Treaty/en/treaties/html/196.htm>.

⁶³En la fecha de preparación del presente documento, los 47 Estados miembros del Consejo de Europa eran los siguientes: Albania, Alemania, Andorra, Armenia, Azerbaiyán, Austria, Bélgica, Bosnia y Herzegovina, Bulgaria, Chipre, Croacia, Dinamarca, Eslovaquia, Eslovenia, España, Estonia, Federación de Rusia, Finlandia, Francia, Georgia, Grecia, Hungría, Irlanda, Islandia, Letonia, antigua República Yugoslava de Macedonia, Liechtenstein, Lituania, Luxemburgo, Malta, República de Moldavia, Mónaco, Montenegro, Noruega, Países Bajos, Polonia, Portugal, República Checa, Reino Unido, Rumanía, San Marino, Serbia, Suecia, Suiza, Turquía y Ucrania.

⁶⁴Véanse Convenio sobre el delito cibernético del Consejo de Europa, art. 36, y Convenio Europeo para la Prevención del Terrorismo, arts. 23 y 24.

cometidos por medio de sistemas informáticos⁶⁵. Este Protocolo adicional también puede facilitar el enjuiciamiento de los actos de terrorismo cometidos por Internet con la intención de incitar a la violencia por motivos de raza, color, ascendencia u origen nacional o étnico, o religión⁶⁶. El Protocolo adicional está abierto a todos los Estados contratantes del Convenio sobre el delito cibernético del Consejo de Europa⁶⁷.

2. Unión Europea

65. En 2002, el Consejo de la Unión Europea adoptó la Decisión marco 2002/475/JAI, de 13 de junio de 2002, sobre la lucha contra el terrorismo, que armoniza la definición de los delitos de terrorismo en todos los Estados miembros de la Unión Europea⁶⁸ mediante la introducción de una definición específica y común del concepto de “terrorismo”, establece normas de competencia para garantizar que los delitos terroristas sean perseguidos de manera eficaz, y esboza medidas concretas con respecto a las víctimas de los delitos de terrorismo. En respuesta a la creciente amenaza terrorista, incluido el uso de nuevas tecnologías, como Internet, en 2008 se modificó la Decisión marco 2002/475/JAI⁶⁹ para incluir específicamente las disposiciones sobre incitación pública a cometer un delito de terrorismo, el reclutamiento para el terrorismo y el adiestramiento de terroristas. En esa decisión, el Consejo de la Unión Europea también tomó nota de la resolución 1624 (2005) del Consejo de Seguridad, en que el Consejo exhortaba a los Estados a que adoptasen medidas a fin de prohibir por ley la incitación a cometer actos terroristas y prevenir las conductas de esa índole.

66. La Decisión marco 2008/919/JAI proporciona una base para perseguir la difusión de propaganda terrorista y la transmisión de conocimientos para la fabricación de bombas también a través de Internet, en la medida en que dicha difusión se haga intencionalmente y cumpla los requisitos de los delitos mencionados. Las enmiendas a la Decisión marco 2002/475/JAI, relativa a los delitos de incitación pública, reclutamiento y adiestramiento se basan en disposiciones similares del Convenio Europeo para la Prevención del Terrorismo⁷⁰. La Decisión marco 2008/919/JAI del Consejo introdujo nuevos delitos referentes a la conducta que puede llevar a cometer actos de terrorismo, independientemente de los medios o instrumentos tecnológicos mediante los cuales se cometan esos delitos. Al igual que lo que sucede con el Convenio Europeo para la Prevención del Terrorismo, si bien las disposiciones de la Decisión marco 2008/919/JAI no se refieren específicamente a Internet, cubren las actividades llevadas a cabo por ese medio.

⁶⁵Consejo de Europa, *European Treaty Series*, núm. 189.

⁶⁶Ibid., art. 2.

⁶⁷Ibid., art. 11.

⁶⁸En la fecha de preparación del presente documento, los 27 Estados miembros de la Unión Europea eran: Alemania, Austria, Bélgica, Bulgaria, Chipre, Dinamarca, Eslovaquia, Eslovenia, España, Estonia, Finlandia, Francia, Grecia, Hungría, Irlanda, Italia, Letonia, Lituania, Luxemburgo, Malta, Países Bajos, Polonia, Portugal, Reino Unido, República Checa, Rumanía y Suecia.

⁶⁹Decisión marco 2008/919/JAI del Consejo de la Unión Europea, de 28 de noviembre de 2008, por la que se enmienda la Decisión marco 2002/475/JAI sobre la lucha contra el terrorismo.

⁷⁰Consejo de Ministros, “Enmienda de la Decisión marco sobre la lucha contra el terrorismo”, comunicado de prensa de 18 de abril de 2008.

3. Otros instrumentos jurídicos

67. A continuación se mencionan otros instrumentos jurídicos vinculantes aprobados por organizaciones regionales o subregionales que pueden contener disposiciones relativas a la lucha contra el uso de Internet con fines terroristas:

- Convención regional sobre la eliminación del terrorismo (1987), de la Asociación de Asia Meridional para la Cooperación Regional
- Convención árabe sobre lucha contra el terrorismo (1998)
- Tratado de Cooperación entre los Estados Miembros de la Comunidad de Estados Independientes para Combatir el Terrorismo (1999)
- Convenio de la Organización de la Conferencia Islámica para la Lucha contra el Terrorismo Internacional (1999)
- Convención sobre la prevención y la lucha contra el terrorismo (1999), de la Organización de la Unidad Africana
- Convención Interamericana contra el Terrorismo (2002)
- Convenio de la Asociación de Naciones de Asia Sudoriental contra el terrorismo (2007)
- Directiva sobre la lucha contra la ciberdelincuencia (2009), de la Comunidad Económica de los Estados de África Occidental.

F. Legislación modelo

68. Pese a que la legislación modelo no crea obligaciones jurídicamente vinculantes, sino que se limita a proporcionar directrices de orientación, desempeña un importante papel en la armonización de las normas jurídicas entre los Estados. A diferencia de las convenciones y los convenios internacionales, que pueden ser objeto de extensas negociaciones para reflejar las necesidades de una amplia gama de posibles signatarios, las disposiciones de las leyes modelo proporcionan a los Estados el beneficio de sólidas disposiciones jurídicas fundamentales como punto de partida para el desarrollo de su legislación interna. Un beneficio clave de la utilización de disposiciones modelo como base de la legislación nacional es la facilitación de la cooperación internacional, en particular mediante la mitigación de los conflictos derivados de la interpretación errónea de las disposiciones de los distintos ordenamientos jurídicos (por ejemplo, entre los países del *common law* y los de tradición romanista) y con respecto a los requisitos de la doble incriminación⁷¹. (Véase un análisis del tema en la sección V. F. 5 *infra*.)

⁷¹De conformidad con el principio de la doble incriminación, la extradición es posible solo en los casos en que el acto en virtud del cual se solicita la extradición sea punible tanto en el Estado requirente como en el Estado requerido.

1. *Commonwealth*

69. La Ley Modelo del Commonwealth sobre delitos informáticos y delitos conexos (2002) se inspiró en el Convenio sobre el delito cibernético del Consejo de Europa⁷². La Ley Modelo procura aprovechar las similitudes entre las tradiciones jurídicas de los Estados miembros del Commonwealth⁷³ para promover la armonización de los aspectos sustantivos y de procedimiento de la lucha contra el delito cibernético y promover la cooperación internacional. La Ley Modelo del Commonwealth está en consonancia con las normas establecidas en el Convenio sobre el delito cibernético del Consejo de Europa.

2. *Comunidad de Estados Independientes*

70. Los Estados miembros de la Comunidad de Estados Independientes (CEI) también han adoptado leyes modelo y directrices destinadas a armonizar los sistemas legislativos nacionales, teniendo en cuenta las experiencias internacionales en la lucha contra el terrorismo. Estas disposiciones modelo reflejan las normas jurídicas internacionales, adaptadas a las necesidades de los Estados miembros de la CEI⁷⁴. Por ejemplo, el artículo 13 de la Ley Modelo sobre el marco reglamentario de Internet⁷⁵ ofrece disposiciones modelo con respecto a la lucha contra el uso de Internet con fines ilícitos.

3. *Unión Internacional de Telecomunicaciones*

71. La Unión Internacional de Telecomunicaciones (UIT) es un organismo especializado de las Naciones Unidas que desempeña un papel rector en la esfera de los delitos cibernéticos. La UIT ha preparado un Manual sobre legislación contra la ciberdelincuencia (2010) para promover la armonización de las legislaciones y normas de procedimiento nacionales sobre la ciberdelincuencia, incluidos los actos de terrorismo cometidos a través de Internet. El manual se preparó a partir de un análisis exhaustivo del Convenio sobre el delito cibernético del Consejo de Europa y la legislación sobre ciberdelincuencia de los países desarrollados⁷⁶. Si bien el Manual de la UIT se ocupa principalmente de cuestiones de seguridad cibernética, presenta disposiciones modelo para la penalización de ciertos actos de terrorismo cometidos utilizando Internet, como

⁷²Para mayor información, véase http://www.thecommonwealth.org/shared_asp_files/uploadedfiles/%7BDA109CD2-5204-4FAB-AA77-86970A639B05%7D_Computer%20Crime.pdf.

⁷³En la fecha de preparación del presente documento, los 53 Estados miembros del Commonwealth eran: Antigua y Barbuda, Australia, Bahamas, Bangladesh, Barbados, Belice, Botswana, Brunei Darussalam, Camerún, Canadá, Chipre, Dominica, Gambia, Ghana, Granada, Guyana, India, Islas Salomón, Jamaica, Kenya, Kiribati, Lesotho, Malasia, Malawi, Maldivas, Malta, Mauricio, Mozambique, Namibia, Nauru, Nigeria, Nueva Zelandia, Pakistán, Papua Nueva Guinea, Reino Unido, República Unida de Tanzania, Rwanda, Saint Kitts y Nevis, Samoa, San Vicente y las Granadinas, Santa Lucía, Seychelles, Sierra Leona, Singapur, Sri Lanka, Sudáfrica, Swazilandia, Tonga, Trinidad y Tabago, Tuvalu, Uganda, Vanuatu y Zambia.

⁷⁴En la fecha de preparación del presente documento, los 11 Estados miembros de la Comunidad de Estados Independientes eran: Armenia, Azerbaiyán, Belarús, Federación de Rusia, Kazajstán, Kirguistán, la República de Moldova, Tayikistán, Turkmenistán, Ucrania y Uzbekistán.

⁷⁵Anexo de la resolución 36-9 de la Asamblea Interparlamentaria de los miembros de la Comunidad de Estados Independientes, aprobada el 16 de mayo de 2011.

⁷⁶Unión Internacional de Telecomunicaciones, Manual sobre legislación contra la ciberdelincuencia (2010), párr. 2.2.

el acceso no autorizado a programas o datos informáticos con fines de terrorismo o la transmisión de software malicioso con la intención de promover el terrorismo⁷⁷.

III. Marcos normativo y legislativo

A. Introducción

72. Además de usar Internet para planear y financiar actos de terrorismo, los terroristas también la utilizan para reclutar y entrenar a nuevos miembros, comunicarse entre sí, investigar o reconocer blancos potenciales, difundir propaganda e incitar a otros a cometer actos de terrorismo.

73. En el presente capítulo se examinan las cuestiones relacionadas con la formulación de las políticas de justicia penal y la legislación encaminadas a combatir esas amenazas, con objeto de determinar, por medio de los ejemplos y las experiencias nacionales ofrecidos por algunos Estados representados en las reuniones del grupo de expertos, cuáles son los problemas y los enfoques comunes que pueden dificultar o fortalecer la investigación y persecución eficaces de los casos de terrorismo relacionados con algún aspecto del uso de Internet.

B. Políticas

74. Con el fin de ofrecer respuestas eficaces de la justicia penal a las amenazas presentadas por los terroristas que usan Internet, los Estados necesitan políticas y marcos nacionales legislativos claros. En términos generales, estas políticas y leyes se centrarán en:

- a) La penalización de los actos ilícitos cometidos por terroristas a través de Internet o servicios conexos;
- b) La dotación de facultades especiales de investigación a los organismos encargados de hacer cumplir la ley que investigan los delitos relacionados con el terrorismo;
- c) La regulación de los servicios relacionados con Internet (por ejemplo, los que prestan los proveedores de servicios de Internet) y el control de contenidos;
- d) La facilitación de la cooperación internacional;
- e) La formulación de procedimientos judiciales o probatorios especializados;
- f) La observancia de las normas internacionales de derechos humanos.

Enfoques normativos

75. En su publicación de 2011, *Proyecto de Informe: «Lucha contra el uso de la Internet para fines terroristas - Aspectos legales»*⁷⁸, el Grupo de Trabajo sobre medidas para hacer

⁷⁸Véase Naciones Unidas, Equipo Especial sobre la Ejecución de la Lucha contra el Terrorismo, Grupo de Trabajo sobre medidas para hacer frente al uso de Internet con fines terroristas, *Proyecto de Informe: «Lucha contra el uso de la Internet para fines terroristas - Aspectos legales»* (Nueva York, 2011).

frente al uso de Internet con fines terroristas del Equipo Especial sobre la Ejecución de la Lucha contra el Terrorismo señaló tres enfoques estratégicos amplios que los Estados podrían adoptar para combatir las actividades terroristas a través de Internet, y que hacen uso de:

- a) Legislación general sobre la ciberdelincuencia;
- b) Legislación general (no específica sobre Internet) contra el terrorismo;
- c) Legislación específica sobre Internet contra el terrorismo.

76. Cabe observar que en el enfoque a), además del empleo de la legislación general sobre ciberdelincuencia, también pueden usarse otros actos delictivos preparatorios como la instigación (*solicitation*) y la asociación ilícita cuando se trabaja con casos de terrorismo que involucran algún aspecto de uso de Internet, en particular cuando se trata de una conducta presunta encaminada a incitar a la comisión de actos de terrorismo.

77. El sistema amplio de clasificación del Grupo de Trabajo es un marco conceptual útil para orientar la labor de los encargados de formular políticas y los legisladores cuando estos consideran los enfoques normativos y legislativos apropiados para sus Estados particulares.

78. Otro recurso útil para los encargados de formular políticas y los legisladores, mencionado en el *Proyecto de Informe: «Lucha contra el uso de la Internet para fines terroristas»*⁷⁹, es el Manual sobre legislación contra la ciberdelincuencia, preparado bajo los auspicios de la UIT. Además de otras disposiciones penales modelo, el Manual trata de varios delitos específicos relacionados con el terrorismo, incluido el artículo 3 f), que trata del acceso no autorizado, o la adquisición de programas informáticos, con el fin de desarrollar, formular, planificar, facilitar o ayudar en la comisión de un delito terrorista, o confabularse para cometer actos de terrorismo.

79. Dentro del amplio marco proporcionado por los instrumentos universales contra el terrorismo y las normas internacionales pertinentes de derechos humanos, los gobiernos tienen una gran flexibilidad para adoptar sus enfoques preferidos; inevitablemente, estos varían de un Estado a otro. En el presente capítulo solo se destacan algunos ejemplos de enfoques adoptados por distintos Estados que podrían ser útiles para los encargados de formular políticas y los legisladores.

80. En la actualidad, son pocos los Estados que han elaborado legislación antiterrorista específicamente destinada a combatir el uso de Internet por los terroristas, pero hay algunos, entre ellos el Reino Unido, donde, después de los atentados de 2005 en Londres, el Gobierno promulgó la Ley de Terrorismo de 2006, parte 1, que contiene disposiciones que tratan específicamente de la actividad basada en Internet que puede alentar o facilitar la comisión de actos de terrorismo. Esta Ley complementa la Ley de uso indebido de computadoras de 1990, que trata de delitos cometidos con computadora y de la ciberdelincuencia en general.

81. En 2007, los Emiratos Árabes Unidos aprobaron leyes cibernéticas federales que, además de penalizar la piratería y otras actividades relacionadas con Internet, penalizan la creación de sitios web o la publicación de información para grupos terroristas con nombres falsos con la intención de facilitar el contacto con sus dirigentes o promover sus ideologías, financiar sus actividades o publicar información sobre cómo fabricar explosivos o preparar otras sustancias para su uso en atentados terroristas⁸⁰.

82. En 2008, el Gobierno de la Arabia Saudita promulgó, entre otras leyes nuevas relacionadas con la tecnología, una ley que tipifica como delito, punible con multa y hasta 10 años de prisión, el poseer un sitio web que promueva o apoye el terrorismo⁸¹.

83. También en 2008, el Gobierno del Pakistán dictó la Ordenanza de prevención de delitos electrónicos, 2008, que contiene disposiciones específicas sobre los delitos relacionados con el terrorismo cibernético. Sin embargo, la ley ya no está en vigor⁸².

84. Por último, ese mismo año, el Gobierno de la India enmendó la Ley sobre la tecnología de la información, de 2000, para incluir el delito de “terrorismo cibernético” (artículo 66F) y otros temas relacionados con Internet.

85. Sin embargo, a nivel internacional, salvo algunas excepciones, a falta de un instrumento universal que imponga expresamente la obligación de promulgar leyes dirigidas específicamente contra las actividades terroristas a través de Internet, la mayoría de los gobiernos han optado por hacer frente a esas amenazas recurriendo a un enfoque ecléctico, es decir, utilizando una combinación de leyes penales generales y leyes específicas sobre ciberdelincuencia y contra el terrorismo. En algunos Estados, por ejemplo, las leyes penales se centran en actos delictivos en sí, sin diferenciar entre los medios específicos por los que se cometen. En este enfoque, se considera que Internet es un mero instrumento mediante el cual los terroristas cometen un delito en sí, previsto muchas veces en las disposiciones del código penal nacional.

86. Este es el enfoque de la República Popular de China, cuyo Código Penal contiene un artículo relativo a la tipificación de todas las actividades ilegales que impliquen el uso de Internet. El artículo 287 del Código Penal tipifica el uso de una computadora en la comisión de un delito, que será perseguido y reprimido de acuerdo con las disposiciones pertinentes del Código. De este modo, en virtud del derecho penal chino, el uso de Internet se considera como un medio o instrumento mediante el cual puede cometerse un acto delictivo, y no como un elemento independiente del delito, y por tanto se penaliza dentro del marco de las disposiciones de fondo del Código Penal.

⁸⁰Ley Federal núm. (2) de 2006 sobre la prevención de delitos basados en la tecnología de la información, *Gaceta Oficial de los Emiratos Árabes Unidos*, vol. 442, 36° año, Muharam 1427 H/enero de 2006 (puede consultarse una traducción oficiosa al inglés en www.aecert.ae/pdfs/Prevention_of_Information_Technology_Crimes_English.pdf).

⁸¹David Westley, “Saudi tightens grip on Internet use”, *Arabian Business*, 26 de enero de 2008.

⁸²“Pakistan lacks laws to combat cyber terrorism”, *The New New Internet*, disponible en www.thenewnewInternet.com/2010/09/01/pakistan-lacks-laws-to-combat-cyber-terrorism.

87. En el contexto del terrorismo, en China hay disposiciones que penalizan distintas formas de actividades terroristas, incluido el artículo 120 del Código Penal, que tipifica las actividades relacionadas con la organización y dirección de organizaciones terroristas o la participación en ellas. Esta amplia disposición de penalización abarca una extensa gama de actividades relacionadas con el terrorismo, incluidas las realizadas a través de Internet.

88. En la República de Corea, hay dos tipos de leyes penales que se pueden aplicar a los actos terroristas cometidos con cierto uso de Internet. Uno de ellos es el código penal general y el otro es un código penal especial, aprobado en 1986, sobre los actos delictivos relacionados con la información o las comunicaciones. El artículo 90 del Código Penal trata de la preparación de esos actos, así como de la confabulación, la incitación o la propaganda y dispone que toda persona que planee o trame cometer delitos en virtud del artículo 87 del Código Penal (disturbios, revueltas o desórdenes públicos) o del artículo 88 (homicidios perpetrados con el fin de cometer alguno de los actos previstos en el artículo 87) será reprimida con prisión de tres años o más. En virtud del artículo 101 del Código Penal, toda persona que prepare o se confabule para cometer cualquiera de los delitos previstos en los artículos 92 a 99 del Código Penal es culpable de un delito y será reprimida con una pena de prisión de dos años o más. El artículo 114 del Código Penal se refiere a la organización de grupos delictivos. También con arreglo al Código Penal especial, el Gobierno estableció una serie de disposiciones que penalizan específicamente los actos ilícitos dirigidos contra las redes de información y comunicaciones o la información personal.

89. En la práctica, independientemente del enfoque normativo adoptado, la experiencia demuestra que la mayoría de los Estados siguen un enfoque polifacético cuando se trata de la investigación y persecución de actos terroristas, incluidos los que suponen cierto uso de Internet. Los organismos encargados de hacer cumplir la ley y las fiscalías utilizan las disposiciones legislativas que mejor se ajustan a las circunstancias particulares de cada caso.

90. Las facultades requeridas por los organismos encargados de hacer cumplir la ley para investigar eficazmente los casos de terrorismo son muy similares, independientemente de la jurisdicción particular de que se trate, y las diferencias existentes en las políticas y leyes nacionales reflejan la diversidad de los ordenamientos jurídicos, las estructuras constitucionales y otros factores (distintas culturas, por ejemplo).

91. La esfera de regulación y control de contenidos de Internet deja amplio margen para las variaciones en los enfoques nacionales. Si bien la Declaración Universal de Derechos Humanos y el Pacto Internacional de Derechos Civiles y Políticos establecen las normas internacionales relativas a la regulación de la expresión y comunicación de ideas, no existe un instrumento amplio, vinculante a nivel internacional, que establezca normas definitivas y vinculantes sobre qué es lo que se considera contenido adecuado de Internet o cómo ha de regular cada Estado las actividades relacionadas con Internet dentro de su propio territorio. En la actualidad, la pornografía infantil es la esfera en que, incluso en ausencia de un instrumento universalmente vinculante o una definición

aceptada, los Estados invariablemente prohíben tales actividades⁸³. En el contexto del terrorismo, empero, la ausencia de una definición universalmente aceptada de terrorismo constituye un obstáculo permanente para cualquier enfoque acordado internacionalmente de una regulación adecuada de las actividades relacionadas con el terrorismo y los contenidos de Internet.

92. En cuanto a los procedimientos judiciales o probatorios especializados en el ámbito del terrorismo, algunos Estados han adoptado procedimientos específicos de gestión judicial y tramitación de las causas de terrorismo que podrían aplicarse a los casos de uso de Internet por los terroristas. Cuando se adopta este enfoque, es importante que los mecanismos especializados se ajusten plenamente a las obligaciones internacionales pertinentes de derechos humanos, incluidas las relacionadas con el derecho a la libertad y a un juicio imparcial.

C. Legislación

1. Penalización

93. Como ya se indicó, ninguno de los instrumentos universales contra el terrorismo impone a los Estados la obligación de promulgar leyes dirigidas específicamente contra la utilización de Internet por los terroristas. En consecuencia, si bien es muy probable que la mayoría de los casos de terrorismo entrañe cierto uso de Internet por los autores, es indudable que en muchos Estados, además de invocar las disposiciones que reprimen la conducta ilícita contenidas en los instrumentos universales, las autoridades también recurrirán a otras disposiciones de sus códigos penales, incluidos los actos delictivos preparatorios como la confabulación, la instigación y la asociación ilícita, a fin de procesar a los delincuentes.

94. En la presente sección, se examinan ejemplos de diferentes disposiciones legislativas de algunos Estados, con el fin de determinar qué enfoques podrían servir de base para una respuesta eficaz de la justicia penal a diferentes tipos de conducta.

a) Uso de Internet para actos o declaraciones de apoyo al terrorismo

95. Además de los actos relacionados con la comisión de actos terroristas en sí (por ejemplo, atentados con bombas), hay pruebas claras de que Internet es usada cada vez más por los terroristas para desarrollar actividades de apoyo, tales como el reclutamiento y adiestramiento de los miembros, el intercambio de información práctica, la difusión de propaganda y la incitación a la comisión de actos de terrorismo. Debido a la configuración y el alcance mundial de Internet, es cada vez más probable que este tipo de actividades sean realizadas por diferentes actores físicamente presentes en distintas jurisdicciones.

⁸³Maura Conway, "Terrorism and Internet governance: core issues", *Disarmament Forum*, vol. 3 (2007), pág. 27.

96. En el Reino Unido, la parte VI de la Ley de Terrorismo de 2000 contiene varias figuras que pueden servir de base para acusar a las personas que se sirven de Internet para apoyar actividades terroristas.

97. El artículo 54 de la Ley tipifica el acto de ofrecer, recibir o invitar a otros a recibir instrucción o entrenamiento en la fabricación o el uso de armas de fuego, sustancias radiactivas o armas conexas, explosivos o armas químicas, biológicas o nucleares.

98. El artículo 57 tipifica la posesión de artículos en circunstancias que den lugar a una sospecha razonable de que la persona que los posee tiene tales artículos en relación con la preparación, instigación a cometer o comisión de un acto de terrorismo. En los últimos años, este artículo se ha invocado para procesar con éxito a varias personas a quienes se encontró en posesión de artículos tan diversos como discos duros, DVD y documentos de instrucción sobre cómo usar artículos tales como morteros, chalecos suicidas y napalm⁸⁴. Para demostrar que se cometió el delito, la fiscalía tiene que probar la existencia de una conexión entre el artículo de que se trate y un acto específico de terrorismo. Si bien se han perseguido con éxito los delitos tipificados en el artículo 57, los tribunales han adoptado un enfoque más restrictivo en la interpretación del ámbito de aplicación del artículo, como lo demuestra la causa *R. c. Zafar, Butt, Iqbal, Raja y Malik* [2008] EWCA Crim 184.

R. c. Zafar, Butt, Iqbal, Raja y Malik

En esta causa de 2007 del Reino Unido, los acusados Zafar, Butt, Iqbal, Raja y Malik apelaron con éxito las sentencias dictadas contra ellos por posesión de artículos con fines relacionados con la comisión o preparación de un acto de terrorismo o instigación a cometerlo, en contravención del artículo 57 de la Ley de Terrorismo de 2000.

Cuatro de los cinco acusados eran estudiantes de la Universidad de Bradford. El quinto, Raja, iba a la escuela en Ilford y había establecido contacto con Iqbal a través del servicio de mensajería de Internet MSN.

Raja visitó Bradford durante unos pocos días y se alojó en la casa en que vivían Iqbal y Zafar. Raja traía consigo tres CD que había hecho y que contenían material seleccionado de la computadora. Llevaban una etiqueta que decía "discos de filosofía". Raja fue detenido por la policía cuando regresaba a su casa después de la visita.

A raíz de investigaciones posteriores, la policía detuvo a los otros acusados y registró sus domicilios, lo cual reveló que ellos también estaban en posesión de material yihadista radical y otros materiales, como un manual militar de los Estados Unidos descargado de Internet. Se encontraron pruebas de comunicaciones a través del servicio de mensajería de Internet, incluida una conversación entre los cuatro recurrentes de Bradford y un primo de Malik, Imran, que vivía en el Pakistán.

⁸⁴Susan Hemming, "The practical application of counter-terrorism legislation in England and Wales: a prosecutor's perspective", *International Affairs*, vol. 86, núm. 4 (julio de 2010), pág. 963.

Originalmente los inculpados fueron acusados en virtud del artículo 58 de la Ley de 2000; sin embargo, en la etapa de instrucción, la fiscalía añadió cargos en virtud del artículo 57, que reflejaban los mismos particulares que los imputados en virtud del artículo 58. Tras varias resoluciones previas al juicio sobre la cuestión de si la información almacenada electrónicamente podía considerarse un artículo a los efectos del artículo 57, la fiscalía optó por proceder al juicio invocando solamente el artículo 57.

En el juicio, Zafar e Iqbal fueron absueltos de un cargo, la posesión de tres “discos de filosofía” que contenían material procedente de Raja; sin embargo, ellos dos, junto con los demás acusados, fueron declarados culpables en relación con todos los demás cargos. Malik fue sentenciado a tres años de prisión, Zafar e Iqbal a tres años de detención en una institución para jóvenes infractores, Butt a 27 meses de detención, y Raja a dos años de detención.

Los acusados apelaron las sentencias. En la apelación, el Tribunal consideró que la cuestión fundamental consistía en saber si, basándose en los hechos del caso, existía una conexión entre los artículos y los actos de terrorismo que cumpliera los requisitos del artículo 57.

Los artículos que los recurrentes poseían, según la fiscalía, en contravención del artículo 57, eran, en su mayor parte, los CD y los discos duros que contenían material almacenado electrónicamente. Este material incluía propaganda ideológica y las comunicaciones entre los acusados, que, según la fiscalía, demostraban la existencia de un plan establecido por los acusados de viajar al Pakistán para recibir entrenamiento y participar en la guerra del Afganistán, lo cual, según la fiscalía, equivalía a cometer actos de terrorismo. El Tribunal de Apelación consideró que la fiscalía tenía que probar primero la finalidad con que cada recurrente poseía el material almacenado y luego que esa finalidad estaba “relacionada con la comisión, preparación o instigación” de futuros actos de terrorismo, que constituía el fundamento de la acusación, es decir, la lucha contra el Gobierno del Afganistán.

Basándose en los hechos del caso, y señalando que estos planteaban difíciles cuestiones de interpretación del ámbito de aplicación del artículo 57, el Tribunal sostuvo que no existía la conexión necesaria, por lo que las condenas resultantes eran inapropiadas, y dio curso a las apelaciones.

99. El artículo 58 de la Ley ha demostrado ser especialmente útil en varios casos en que las autoridades han tenido que intervenir cuando no había pruebas de que el imputado se dedicara a actividades asociadas con el terrorismo. El artículo tipifica el acto de reunir, hacer o poseer, sin causa justificada, cualquier documento o registro con información de un tipo que pueda ser útil a una persona que cometa o prepare la comisión de un acto terrorista, o poseer cualquier documento o registro que contenga dicha información.

100. En *R c. K* [2008] 3 All E.R. 526, el Tribunal sostuvo que un documento entra en el ámbito de aplicación del artículo 58 solo si es de un tipo que se preste para proporcionar asistencia práctica a una persona que cometa o prepare la comisión de un acto de terrorismo. Este enfoque fue reafirmado en *R c. G y J* [2009] UKHL 13, en que el Tribunal reafirmó este “criterio de la utilidad práctica”, según el cual la posesión de un documento o registro es un delito solo si es de utilidad práctica y si

la persona que lo posee no tiene una causa justificada⁸⁵. No hay ninguna restricción a lo que puede constituir una causa justificada para este fin, siempre que se pueda invocar como defensa ante un tribunal.

101. Con arreglo al artículo 58, el fiscal no está obligado a probar que el acusado sea un terrorista o que los artículos que posee los tenga con fines terroristas; sin embargo, la fiscalía puede, solo en circunstancias muy limitadas, recurrir a pruebas extrínsecas para demostrar la utilidad práctica de cualquier artículo. Por ejemplo, pueden presentarse pruebas de cifrado para descifrar un documento escrito en clave, pero no pueden presentarse pruebas para explicar el significado de lugares marcados en un mapa. La información debe “hablar por sí misma” y no ser de tipo general.

102. En *R. c. Sultán Mohammed* [2010] EWCA Crim 227, el tribunal sostuvo que “siempre que el documento que contiene la información no sea de uso diario por los miembros ordinarios del público (por ejemplo, horarios y mapas publicados) y siempre que un jurado razonable pueda concluir correctamente que la información que contiene el documento es de un tipo tal que podría ser útil para una persona que cometa o prepare la comisión de un acto de terrorismo, solo entonces podrá el jurado decidir si está convencido de que el documento contiene dicha información. En tal caso, y siempre que el acusado tenga la necesaria intención dolosa, la única cuestión será decidir si el acusado tiene una causa justificada”⁸⁶. El jurado deberá decidir en consecuencia si la explicación dada para justificar la posesión del documento es en realidad razonable, teniendo en cuenta los hechos y las circunstancias particulares de cada caso⁸⁷.

103. La Ley de Terrorismo de 2006 tipificó (en su artículo 5) la “comisión de actos en preparación de actos de terrorismo”. Este artículo fue concebido para incriminar a aquellas personas que preparan activamente la comisión de actos de terrorismo pero son detenidas antes de cometer o intentar cometer un acto terrorista en sí⁸⁸.

104. El artículo 5 ha sido particularmente útil en los casos de delincuentes que actúan solos y no hay pruebas suficientes para fundamentar un cargo de confabulación, ya que no se puede demostrar que haya participado más de una persona en el delito o las autoridades no conocen en detalle el delito que se estaba planeando cometer. La figura delictiva no exige prueba de que se haya cometido, en definitiva, un acto o actos de terrorismo, pero la acusación debe probar la intención específica de cometer un acto terrorista o de ayudar a otros a cometerlo. En el Reino Unido se ha condenado a varias personas por este delito, a las que se impusieron diversas penas de prisión, incluida la cadena perpetua⁸⁹.

⁸⁵Ibid., pág. 962.

⁸⁶Cita tomada de “R. c. Muhammed [2010] EWCA Crim 227: terrorism - preparing an act of terrorism”, *Criminal Law and Justice Weekly* (20 de marzo de 2010).

⁸⁷Hemming, “The practical application of counter-terrorism legislation in England and Wales”, pág. 963.

⁸⁸Ibid., pág. 964.

⁸⁹Ibid.

105. La causa *R c. Terence Roy Brown* [2011] EWCA Crim 2751 es un buen ejemplo de la utilidad de disposiciones tales como la del artículo 58.

R c. Terence Roy Brown

Terence Roy Brown, ciudadano del Reino Unido, tenía un negocio en línea, que consistía en anunciar y vender una edición anual de un CD-ROM que él llamaba "Anarchist's Cookbook" (Libro de Cocina del Anarquista), título casi idéntico al de otro libro muy conocido llamado *The Anarchist Cookbook*. En lugar de una sola publicación, no obstante, estos discos contenían 10.322 ficheros, algunos de los cuales eran publicaciones completas por sí solas. Estas incluían manuales terroristas, como el Manual de Al-Qaida, e instrucciones para la fabricación de diferentes tipos de explosivos y la construcción de bombas. Otros ficheros consistían en instrucciones para preparar venenos, cómo evitar atraer la atención de las autoridades durante los viajes, y técnicas de manejo de armas. En un aparente intento de soslayar la ley, el Sr. Brown publicó en el sitio web donde anunciaba su publicación un descargo de responsabilidad, indicando que las instrucciones que contenían podrían ser ilegales o peligrosas si se ponían en práctica y que perseguían exclusivamente fines "de lectura recreativa y de interés histórico". La investigación dejó en claro que el Sr. Brown obraba motivado puramente por incentivos comerciales. También se hizo evidente que había ampliado su colección en el período inmediatamente posterior a los atentados de Londres de julio de 2005 y, como resultado de ello, había aumentado considerablemente sus ganancias.

En marzo de 2011, el Sr. Brown fue declarado culpable de siete cargos con arreglo a la Ley de Terrorismo de 2000 (artículo 58) en relación con la reunión de información que podría haber sido utilizada para preparar o cometer actos de terrorismo, dos cargos con arreglo a la Ley de Terrorismo de 2006 (artículo 2) en relación con la difusión de publicaciones terroristas y un cargo en virtud de la Ley del producto del delito, de 2002, relacionado con la transferencia de bienes producto de delitos (el uso por el imputado de las ganancias de su negocio)^a.

La excusa alegada por el Sr. Brown en el juicio fue que sus actividades no representaban más que el ejercicio legítimo de su derecho a la libertad de expresión en relación con el material que estaba libremente disponible en Internet y que era similar en tipo, si no en volumen, al que vendían otras librerías en línea. Se adujeron los mismos argumentos en una solicitud de apelación de la sentencia, que no tuvo éxito. El tribunal resolvió que la restricción de los derechos del Sr. Brown, conforme al artículo 10, en relación con el material que probablemente podría ayudar a los terroristas, estaba justificada y era proporcionada. El tribunal también confirmó que la fiscalía estaba facultada para no acusar a cada persona que pudo haber cometido un delito y considerar, en cambio, cada caso por sí mismo.

^a"Businessman who published bomb-makers' handbook 'facing lengthy spell in jail'", *Daily Mail*, 9 de marzo de 2011. Puede consultarse en www.dailymail.co.uk/news/article-1364621/Businessman-published-bomb-makers-handbook-facing-lengthy-spell-jail.html#ixzz1j4gXbMLu.

106. Esta causa es una entre varias, incluida la causa *R c. K* [2008] QB 827 y *R c. G* [2010] 1 AC 43, en que los tribunales del Reino Unido aclararon la doctrina legal en cuanto al alcance y la aplicación del artículo 58 de la Ley, a la luz de las garantías pertinentes de los derechos humanos.

107. Además de los delitos previstos en la legislación antiterrorista, las autoridades del Reino Unido han invocado, cuando las circunstancias así lo aconsejaban, el delito de instigación para procesar con éxito a personas que llevaban a cabo actividades relacionadas con el terrorismo. Ejemplo de este enfoque es la causa *R c. Bilal Zaheer Ahmad*⁹⁰, en que el acusado fue declarado culpable de instigación de homicidio.

R c. Bilal Zaheer Ahmad

Esta causa del Reino Unido está vinculada a otra causa que la precedió, la de Roshanara Choudhry, de 2010, condenada a cadena perpetua el 2 de noviembre de 2010, por tentativa de homicidio de Stephen Timms, miembro del Parlamento.

En una declaración, Choudhry dijo que había decidido cometer el delito unas cuatro semanas antes del ataque, en mayo de 2010, y había comprado dos cuchillos en preparación del ataque, uno como repuesto en caso de que el primero se rompiera mientras apuñalaba a la víctima. Choudhry dijo a la policía que había estado mirando videos de Anwar al-Awalaki y Abdullah Azzam y había visitado el sitio web www.revolutionmuslim.com durante su período de radicalización. Este conocido sitio, hospedado en los Estados Unidos, contenía material de promoción de la yihad violenta, incluidos videos y arengas que alentaban el terrorismo y enlaces web con publicaciones terroristas.

El 1 de noviembre de 2010, el acusado publicó un enlace en su página de Facebook con un reportaje sobre el caso Timms/Choudhry, al que añadió el siguiente comentario:

Esta hermana nos ha avergonzado a los hombres. NOSOTROS TENDRÍAMOS QUE ESTAR HACIENDO ESO.

El 4 de noviembre de 2010, el acusado publicó un artículo titulado “Los miembros del Parlamento que votaron a favor de la guerra en el Iraq”, en el sitio web de la Revolución Musulmana con el nombre de “BILAL”. El artículo estaba encabezado por el símbolo del Estado Islámico del Iraq (facción de Al-Qaida) y comenzaba con una cita del Corán según la cual quienes mueren sin haber participado en la yihad son unos hipócritas.

El artículo informaba a los lectores de que podían “seguir los pasos” de los miembros del Parlamento británico a través de un enlace, que citaba, con un sitio web oficial del Parlamento. Esto les permitiría conocer los detalles del lugar donde algún miembro del Parlamento se sometería a una operación quirúrgica, por ejemplo, donde podrían “encontrarlo en persona”.

A esto seguían 29 citas de pasajes religiosos, traducidos al inglés y todo lo relativo a la obligación de los musulmanes de participar en la yihad o buscar el “martirio”. Inmediatamente a continuación de las citas figuraba un enlace con un sitio web que anunciaba un cuchillo para la venta. Los agentes británicos encargados de la lucha contra el terrorismo obtuvieron una copia de este artículo para usarlo con fines probatorios. Se obtuvo una copia adicional de la página web de Google Inc. en respuesta a una comisión rogatoria.

El 10 de noviembre de 2010, el acusado fue detenido por la Unidad contra el Terrorismo de la Policía de West Midlands, cerca de su casa en Wolverhampton. Se le encontró en posesión de una computadora portátil, que, según declaró a los agentes que lo detuvieron, había utilizado para publicar el artículo sobre los parlamentarios en el sitio web de la Revolución Musulmana. El examen forense de la computadora portátil reveló que el sospechoso parecía haber intentado borrar los rastros de sus actividades en línea antes de ser detenido.

El 16 de noviembre, el imputado fue acusado de instigar al homicidio en relación con el artículo publicado y de tres delitos de posesión de material que podría ser de utilidad a un terrorista en virtud del artículo 58 de la Ley de Terrorismo de 2000. Más tarde el imputado se declaró culpable de estos delitos, así como de un delito de incitación al odio religioso, por unos comentarios que había hecho en un foro de Internet, y fue condenado a 12 años de prisión, con otros cinco años de libertad vigilada.

108. En los Estados Unidos, el Título 18 del Código de los Estados Unidos, artículo 842 *p*), titulado “Distribución de información relativa a explosivos, artefactos destructivos y armas de destrucción en masa”, tipifica el acto de distribuir, por cualquier medio, información sobre la fabricación o el uso de explosivos, artefactos destructivos o armas de destrucción en masa con la intención de que la información sea utilizada para facilitar la comisión de un delito violento, o a sabiendas de que la persona a la que se distribuye la información tiene la intención de utilizar la información para facilitar la comisión de un delito violento. Esta ley se ha invocado en los Estados Unidos para procesar a personas que habían distribuido información de ese tipo por Internet.

b) Incitación

109. El delito de incitación a cometer actos terroristas es el tema de la resolución 1624 (2005) del Consejo de Seguridad. En esa resolución, el Consejo instó a todos los Estados a que, entre otras cosas, adoptaran las medidas necesarias y adecuadas en cumplimiento de sus obligaciones de derecho internacional para prohibir por ley la incitación a la comisión de un acto o actos de terrorismo, y para impedir dicha conducta.

110. El desarrollo y la aplicación de leyes que penalizan la incitación a cometer actos de terrorismo, sin dejar por ello de proteger plenamente, al mismo tiempo, los derechos humanos tales como el derecho a la libertad de expresión y de asociación, presentan un desafío permanente para los encargados de formular políticas, los legisladores, las entidades responsables de hacer cumplir la ley y los fiscales. Los casos de declaraciones hechas por personas a través de Internet, sobre todo cuando el autor de las declaraciones, los servicios de Internet utilizados y sus destinatarios se encuentran en diferentes jurisdicciones y se rigen por diferentes leyes nacionales y garantías constitucionales, presentan problemas adicionales para los investigadores y fiscales desde el punto de vista de la cooperación internacional.

111. La experiencia internacional en relación con la persecución de los delitos relacionados con la incitación a cometer actos terroristas pone de relieve dos cuestiones: en primer lugar, lo importante (y a veces difícil) que es en la práctica distinguir entre

propaganda terrorista (declaraciones en favor de determinadas opiniones ideológicas, religiosas o políticas) y materiales o declaraciones que constituyen incitación a cometer atentados terroristas y, en segundo lugar, la necesidad de evaluar cuidadosamente, caso por caso, las circunstancias y el contexto de cada uno, antes de invocar las leyes aplicables a presuntos actos de incitación, para determinar si procede la institución de un juicio por el delito de incitación en un caso particular.

112. Los miembros del grupo de expertos que habían participado en casos relacionados con la investigación y persecución de delitos de incitación a la comisión de actos terroristas estuvieron de acuerdo y destacaron la importancia, en la práctica, de evaluar plenamente el contexto en que se habían hecho las presuntas declaraciones de incitación, teniendo en cuenta no solo las palabras, sino también el foro en que se habían hecho, y sostuvieron que las características de los destinatarios probables podrían ser factores muy pertinentes para determinar, en un caso particular, si convenía iniciar un proceso penal por el delito de incitación y, en caso de hacerlo, las probabilidades de éxito.

113. En el Reino Unido, el artículo 59 de la Ley de Terrorismo de 2000 tipifica el acto de incitar a otra persona a cometer un acto de terrorismo, en todo o en parte, fuera del Reino Unido, cuando el hecho, de haberse perpetrado en Inglaterra y Gales, constituiría un delito especificado en el artículo (por ejemplo, homicidio, lesiones intencionales, explosiones o daños a los bienes que pongan en peligro la vida).

114. En el conocido caso de *R. c. Tsouli y otros*⁹¹, Younes Tsouli, Mughal Waseem y Tariq al-Daour se declararon culpables de los cargos formulados en virtud de la Ley de Terrorismo de 2000, de incitar al homicidio con fines terroristas mediante el establecimiento y mantenimiento de un gran número de sitios web y foros de charla utilizados para publicar materiales que incitaban a cometer actos terroristas de homicidio, principalmente en el Iraq.

R c. Tsouli y otros

Este conocido caso del Reino Unido se refiere a tres acusados —Younes Tsouli, Mughal Waseem y Tariq al-Daour— contra quienes se formularon inicialmente 15 cargos. Antes del juicio, Tsouli y Mughal se declararon culpables de un cargo de confabulación para cometer fraude. Durante el juicio, después de escuchar las pruebas de cargo, los tres se declararon culpables del cargo de incitar al terrorismo en el extranjero, y Al-Daour se declaró culpable de un cargo de confabulación para cometer fraude.

Entre junio de 2005 y su detención en octubre de 2005, los acusados habían estado abocados a la compra, construcción y mantenimiento de gran número de sitios web y foros de charla de Internet donde publicaban material que incitaba a cometer actos terroristas de homicidio, principalmente en el Iraq. El costo de adquisición y mantenimiento de los sitios web se sufragaba con el producto del fraude de tarjetas de crédito. El material de los sitios web contenía declaraciones de que era el deber de los musulmanes emprender la yihad

armada contra los judíos, los cruzados, los apóstatas y sus partidarios en todos los países musulmanes y que era deber de todo musulmán luchar con ellos y matarlos, dondequiera que estuviesen, fueran civiles o militares.

En los foros de charla de Internet, se proporcionaban a las personas dispuestas a unirse a la insurgencia las rutas para viajar al Iraq y manuales de instrucciones sobre armas y explosivos. En el domicilio de cada acusado se encontró material ideológico extremista que demostraba la adhesión a la justificación declarada de los actos de homicidio a los que se incitaba en los sitios web y foros de charla.

Al-Daour organizó la obtención de tarjetas de crédito robadas, tanto para sus propios fines como para proporcionar fondos a Mughal para la creación y el funcionamiento de los sitios web. Al-Daour también había estado implicado en otras operaciones fraudulentas de tarjetas de crédito, pero el producto de esas operaciones no se destinaba al apoyo de los sitios web. Las pérdidas sufridas por las empresas de tarjetas de crédito debidas a este aspecto de las actividades fraudulentas de los acusados ascendían a 1,8 millones de libras esterlinas.

Entre las pruebas figuraba una lista de puño y letra de Tsouli, que se encontró en su escritorio, en la que había escrito los detalles de una serie de sitios web y de las tarjetas de crédito robadas. Se enumeraban en ella 32 sitios web independientes proporcionados por varias empresas diferentes de hospedaje de Internet que Tsouli había establecido o tratado de establecer, en su mayoría en la última semana de junio de 2005, pero había continuado esta tarea en julio y agosto. La creación y administración de estos sitios web se financiaban con el producto del uso fraudulento de los datos de las tarjetas de crédito que habían sido robados de los titulares de cuentas, ya sea por robo directo de los registros informáticos, por piratería o por alguna desviación fraudulenta dentro de las instituciones financieras. Estos datos de las tarjetas de crédito habían sido transmitidos a Tsouli por los otros dos acusados.

Los sitios web creados por Tsouli fueron utilizados como vehículo para la carga de materiales yihadistas, que incitaban a cometer actos de violencia fuera del Reino Unido, en el Iraq. El acceso a los sitios estaba restringido a las personas que habían recibido nombres de usuario y contraseñas. Esto obedecía, según concluyó el juez de primera instancia, al deseo de hacer que fuera más difícil para las empresas de hospedaje de Internet y los organismos encargados de hacer cumplir la ley enterarse de lo que se publicaba en esos sitios.

El 5 de julio de 2007, Tsouli fue condenado a 10 años de prisión y 3 años y medio (pena concurrente) por dos cargos, Mughal, a 7 años y medio de prisión y 3 años y medio (pena concurrente) por dos cargos, y Al-Daour, a 6 años y medio de prisión y 3 años y medio (pena concurrente).

115. La Parte 1 de la Ley de Terrorismo de 2006 estableció una serie de nuevos delitos para facilitar la intervención de las autoridades en los casos de declaraciones de personas que incitan a cometer actos de terrorismo o los glorifican, o tienden de algún modo a apoyar la comisión de tales actos

116. La Parte 1 de la Ley tipifica el acto de publicar una declaración con la intención de alentar, directa o indirectamente, a miembros del público a preparar, instigar o cometer actos de terrorismo, incluidas las expresiones de aliento (pero sin limitarse a ello) que “glorifican” los actos terroristas, o ese mismo acto cometido por imprudencia en cuanto a las consecuencias de esa conducta. En la práctica, la interpretación

probable de una declaración de este tipo tenderá a basarse en el contenido en su conjunto y en el contexto en que se difunde.

117. En el artículo 2 de la Ley se tipifica la difusión (intencional o por imprudencia) de publicaciones terroristas. Estas se definen como las publicaciones que tienden a fomentar los actos de terrorismo o que puedan ser de utilidad a alguien que prepare la comisión de tal acto o lo cometa. Esta segunda categoría abarca los mismos tipos de documentos o publicaciones a los que se aplica el artículo 58 de la Ley de Terrorismo de 2000. Al igual que lo que sucede con el artículo 1 de la Ley de Terrorismo de 2006, la cuestión de si el material en cuestión corresponde a la definición de “publicación terrorista” debe determinarse en función de su contenido en su conjunto y el contexto en que se difunde⁹².

118. En el Reino Unido, cuando los fiscales consideran la posibilidad de iniciar procesos por incitación, ejercen amplia discreción, teniendo en cuenta el derecho a la libertad de expresión y el contexto global en el que se hicieron y difundieron las declaraciones o publicaciones, incluida la forma en que era probable que fueran interpretadas, tanto por el público en general como por los destinatarios.

119. En los Estados Unidos, se sigue un enfoque jurídico diferente respecto de la penalización y persecución de los actos de incitación al terrorismo debido a las garantías constitucionales que protegen el derecho a la libertad de expresión con arreglo a la Primera Enmienda de la Constitución. En virtud de los principios establecidos en el caso histórico de *Brandenburg c. Ohio*, 395 US. 444 (1969), con el fin de procesar con éxito a una persona por instigación de actos delictivos (incluido el terrorismo), la Fiscalía tiene la obligación de probar tanto la intención de incitar a la comisión de un acto ilícito o de cometerlo como la probabilidad de que la declaración incite efectivamente a cometer un acto ilícito inminente⁹³.

120. En la persecución de declaraciones que incitan a cometer actos de terrorismo, las autoridades de los Estados Unidos recurren a los actos delictivos preparatorios tales como la instigación (*solicitation*) y la confabulación, junto con las disposiciones sobre “apoyo esencial” del Código Penal de los Estados Unidos, que en ciertas circunstancias permiten el enjuiciamiento de conductas de apoyo a actos violentos de terrorismo⁹⁴.

121. Las disposiciones sobre apoyo esencial, material o de otra índole, del Código Penal de los Estados Unidos, Título 18, artículos 2339A y 2339B, prohíben a toda persona proporcionar, intentar proporcionar o confabularse para proporcionar, a sabiendas o intencionalmente, apoyo o recursos esenciales, materiales o de otra índole, a una organización terrorista. La Ley USA PATRIOT (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) de 2001

⁹²Hemming, “The practical application of counter-terrorism legislation in England and Wales”, pág. 963.

⁹³Elizabeth M. Renieris, “Combating incitement to terrorism on the Internet: comparative approaches in the United States and the United Kingdom and the need for an international solution”, *Vanderbilt Journal of Entertainment and Technology Law*, vol. 11, núm. 3 (2009), págs. 681 y 682.

⁹⁴Código Penal de los Estados Unidos, título 18, artículos 2339A y 2339B.

amplió la definición de apoyo esencial, material o de otra índole, para incluir “cualquier bien, tangible o intangible, o servicio, incluidos ... el adiestramiento, el asesoramiento o la asistencia especializados o ... equipo de comunicaciones”⁹⁵.

122. Las disposiciones sobre los delitos de instigación o confabulación, que figuran en el Código Penal de los Estados Unidos, Título 18, artículo 373 a), establecen que podrá ser acusada de instigación cualquier persona que “instigue, ordene, induzca o procure de otra manera persuadir a otra persona que incurra en una conducta delictiva con la intención de que otra persona incurra en esa conducta”.

123. En los Estados Unidos, ha habido varios casos en que se ha adoptado este enfoque para procesar con éxito a terroristas por lo que habían dicho o hecho por Internet. Cabe mencionar, entre otras, la causa *Estados Unidos de América c. Emerson Winfield Begolly*.

Estados Unidos de América c. Emerson Winfield Begolly

Un estudiante de 22 años (de nacionalidad estadounidense), Emerson Winfield Begolly, fue acusado de participación en la distribución por Internet de información sobre la fabricación de bombas y de instigación para cometer actos de violencia en territorio norteamericano. Los cargos adicionales en su contra incluían el haber agredido y amenazado a agentes de la Oficina Federal de Investigación (FBI) con un arma de fuego cargada.

Formalmente conocido por el alias de “Asadullah Alshishani”, Begolly participó activamente en un foro yihadista de fama internacional llamado Ansar al-Mujahideen English Forum y con el tiempo se convirtió en un moderador activo. El foro brindaba a Begolly la oportunidad de expresar su afinidad con ideas radicales, al tiempo que alentaba a otros miembros de su fe a participar en actos terroristas dentro de los Estados Unidos. Su propaganda consistía, entre otras cosas, en la difusión de videos con instrucciones para fabricar artefactos explosivos para cometer atentados terroristas. Los blancos previstos incluían sinagogas, instalaciones militares, líneas de ferrocarril, comisarías, puentes, torres de teléfonos celulares y plantas de tratamiento de agua.

Durante nueve meses, Begolly publicó varios mensajes extensos en los que examinaba detenidamente la necesidad de violencia. Una acusación formal emitida el 14 de julio de 2011 por el Tribunal del Distrito Este de Virginia, de los EE.UU., contenía como elemento probatorio clave parte de la propaganda que Begolly había publicado en un foro de Internet:

Las protestas pacíficas no funcionan. Los kuffara ven la guerra como la solución de sus problemas, por lo que nosotros tenemos que ver la guerra como solución de los nuestros. No hay paz. Solo balas, bombas y operaciones martirio.

También publicó enlaces de remisión a un documento en línea titulado “Curso sobre explosivos”, disponible para su descarga. El documento, de 101 páginas y escrito por “el mártir Jeque profesor Abu Khabbab al Misri” (tal como lo llamaba Begolly), contiene

⁹⁵Renieris, “Combating incitement to terrorism on the Internet”, págs. 682 y 683.

instrucciones detalladas sobre la instalación de un laboratorio de química con los componentes básicos para la fabricación de explosivos. Se agregaba una nota en la que se advertía a los que descargarán el contenido que debían tener cuidado de usar software de anonimato para su propia seguridad.

Durante todo este tiempo, Begolly había estado bajo la vigilancia constante de las autoridades federales. Un agente del FBI descargó el documento de uno de los enlaces publicados, lo que en definitiva llevó a la detención de Begolly. El 14 de abril de 2011, fue acusado de distribución ilegal y deliberada de información por Internet relacionada con la fabricación y distribución de materiales explosivos y el uso de armas de destrucción en masa, y de instigación para cometer atentados con bombas en lugares de uso público, edificios gubernamentales e instalaciones de transporte público. El 9 de agosto de 2011, Begolly se declaró culpable de instigación para cometer actos terroristas. Actualmente espera sentencia.

^aTérmino muy utilizado por Begolly durante sus discusiones en los foros en línea para referirse a los “no creyentes” o infieles.

c) *Examen del enfoque jurídico de la incitación*

124. En Europa, el artículo 3 de la Decisión marco 2008/919/JAI del Consejo de la Unión Europea, de 28 de noviembre de 2008, que modifica la Decisión marco 2002/475/JAI sobre la lucha contra el terrorismo, y el artículo 5 del Convenio Europeo para la Prevención del Terrorismo, del Consejo de Europa, obligan a los Estados partes en cada instrumento a penalizar los actos o las declaraciones que constituyen incitación a cometer actos de terrorismo. El Convenio Europeo para la Prevención del Terrorismo impone a los Estados miembros la obligación de tipificar “la incitación pública a cometer un delito de terrorismo”, así como el reclutamiento y adiestramiento de terroristas.

125. La aplicación del Convenio, que se basa en parte en el artículo 3 del Protocolo adicional al Convenio sobre la ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos, obliga a los Estados a establecer un equilibrio razonable entre los requisitos de aplicación de la ley y la protección de los derechos humanos y las libertades. Por esta razón, ha dado lugar a serias preocupaciones y debates. Sin embargo, el artículo 5 (al igual que los artículos 6 y 7 sobre el reclutamiento y adiestramiento con fines terroristas) debe aplicarse junto con la disposición básica del artículo 12, según el cual la aplicación de la penalización debe llevarse a cabo de manera que respete los derechos humanos y, en particular, los derechos a la libertad de expresión, la libertad de asociación y la libertad de religión, tal y como se establece en los instrumentos de derechos humanos, incluido el artículo 10, párrafo 1, del Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales.

126. El Tribunal Europeo de Derechos Humanos, en la evaluación de la protección otorgada por el artículo 10, párrafo 1, del Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales, ya se ha ocupado del artículo 5 del Convenio Europeo para la Prevención del Terrorismo. En el conocido caso de *Leroy*

c. *Francia*⁹⁶, un tribunal francés concluyó que no había habido violación del artículo 10 en el caso de un periodista que había sido condenado y multado por publicar una caricatura en un semanario vasco. El 11 de septiembre de 2001, el dibujante presentó al equipo editorial de la revista un dibujo que representaba el ataque contra las torres gemelas del World Trade Centre, con una leyenda que parodiaba el lema publicitario de una marca famosa: “Todos hemos soñado con eso ... ¡Hamás lo hizo realidad!” (“¡Sony lo hizo realidad!”). El dibujo fue publicado en la revista el 13 de septiembre de 2001.

127. En su razonamiento, el Tribunal Europeo de Derechos Humanos se remitió, entre otras cosas, al artículo 5 del Convenio Europeo para la Prevención del Terrorismo, y esta fue la primera vez que el Tribunal tuvo en cuenta el Convenio en un juicio. El Tribunal sostuvo que el dibujo iba más allá de una simple crítica de los Estados Unidos, pues apoyaba y glorificaba su destrucción violenta. El Tribunal señaló que la leyenda que acompañaba al dibujo indicaba el apoyo moral del recurrente a los presuntos autores de los atentados del 11 de septiembre de 2001. Otros factores que tuvo en cuenta el Tribunal fueron las palabras elegidas por el recurrente, la fecha de publicación de los dibujos (factor que, a juicio del Tribunal, aumentaba la responsabilidad del dibujante) y la región —con una situación política delicada— en que se había distribuido (el País Vasco). Según el Tribunal, la caricatura había provocado cierta reacción del público, capaz de incitar a la violencia y tener un efecto considerable en el orden público de la región. Los principios desarrollados en este caso histórico se aplicarán igualmente a los casos en que la supuesta incitación al terrorismo se haya hecho por Internet.

128. En Europa se han procesado con éxito actos de incitación. Por ejemplo, en Alemania, en 2008, Ibrahim Rashid, inmigrante kurdo iraquí, fue declarado culpable de incitación tras ser acusado de librar una “yihad virtual” en Internet. Los fiscales alegaron que, al publicar propaganda de Al-Qaida en las salas de charla de Internet, Rashid estaba tratando de conseguir reclutas para unirse a Al-Qaida y participar en la yihad.

129. El *Compendio de casos relativos a la lucha contra el terrorismo*, de la UNODC⁹⁷, contiene un resumen útil de los criterios adoptados para la penalización de los actos de incitación en Argelia, Egipto, España y el Japón. En Argelia, el artículo 87 bis 1 del Código Penal reprime los actos violentos de terrorismo con la pena de muerte, cadena perpetua o largas penas de prisión. El artículo 87 bis 4 establece que todo aquel que justifique, aliente o financie cualquiera de los actos terroristas enumerados en una lista será reprimido con pena de prisión de 5 a 10 años, y una multa⁹⁸.

130. En Egipto, el artículo 86 bis del Código Penal, tipifica como delitos los actos que entrañen responsabilidad de ejecución y apoyo, la planificación y preparación de actos terroristas, la pertenencia o el apoyo a una organización ilegal, la aportación de

⁹⁶Fallo del Tribunal Europeo de Derechos Humanos (quinta sección), causa *Leroy c. Francia*, Application no. 36109/03, de 2 de octubre de 2008.

⁹⁷Oficina de las Naciones Unidas contra la Droga y el Delito, *Compendio de casos relativos a la lucha contra el terrorismo* (2010).

⁹⁸*Ibid.*, párr. 100.

apoyo financiero y material a organizaciones terroristas y los actos de incitación. Por otra parte, el artículo establece penas agravadas, entre otras cosas, para la promoción deliberada (por cualquier medio) de los fines de organizaciones terroristas o para la obtención o producción (directa o indirecta) de artículos, publicaciones o grabaciones de cualquier tipo destinados a promover o fomentar tales fines⁹⁹.

131. En el Japón, cualquier persona que induzca a cometer un delito, directamente o por un intermediario, está sujeta a la misma pena que si hubiera sido uno de los autores materiales del delito (artículo 61 del Código Penal)¹⁰⁰. Otras disposiciones legales del Japón, tales como los artículos 38 a 40 de la Ley de prevención de actividades subversivas, tipifican la incitación a la insurrección o incendio intencional, con ánimo de promover, apoyar u oponerse a cualquier doctrina o normativa política.

132. En España, los artículos 18 y 579 del Código Penal español hacen de la incitación pública a cometer un delito de terrorismo un acto preparatorio del delito de provocación. El artículo 578 castiga el delito de enaltecimiento del terrorismo, delito que se incorporó en el Código Penal por la Ley Orgánica 7/2000, de 22 de diciembre de 2000. Este artículo establece que “El enaltecimiento o la justificación por cualquier medio de expresión pública o difusión de los delitos comprendidos en los artículos 571 a 577 de este Código o de quienes hayan participado en su ejecución, o la realización de actos que entrañen descrédito, menosprecio o humillación de las víctimas de los delitos terroristas o de sus familiares se castigará con la pena de prisión de uno a dos años”. La Ley Orgánica también impone una pena de un período de incapacidad civil, en caso de condena¹⁰¹.

133. En Indonesia no existe legislación específica sobre las actividades terroristas por Internet, incluida la incitación a cometer actos de terrorismo. El artículo 14 de la Ley núm. 15/2003 sobre la eliminación de los actos de terrorismo trata de la incitación a cometer actos terroristas pero sin hacer referencia a la forma particular de comunicación utilizada por el autor, al igual que el Código Penal indonesio, que aborda la incitación a cometer otros actos delictivos. Las autoridades indonesias han enjuiciado con éxito a personas acusadas de desarrollar actividades relacionadas con el terrorismo por Internet. En 2007, Agung Prabowo, también conocido como Max Fiderman, de 24 años de edad, fue condenado a tres años de prisión (de conformidad con el artículo 13 c) del Reglamento del Gobierno que reemplazó a la Ley núm. 1/2002 y la Ley núm. 15/2003, sobre la eliminación de los actos de terrorismo) por registrar y hospedar un sitio web, www.anshar.net, a petición de Noordin M. Top, cabecilla del grupo terrorista Jemaah Islamiyah, por conducto de un intermediario, Abdul Aziz. Según se informa, Aziz había diseñado el sitio web www.anshar.net a mediados de 2005, a petición de Top, con objeto de difundir propaganda yihadista. Si bien contenía información general sobre el Islam y la yihad, también contenía “instrucciones y consejos” concretos sobre cómo y dónde llevar a cabo ataques terroristas, y sugería rutas de acceso a centros comerciales y

⁹⁹Ibid., párr. 111.

¹⁰⁰Ibid., párr. 100.

¹⁰¹Ibid., párr. 115.

oficinas, atascos de vehículos y otros lugares, mencionados explícitamente, donde podían reunirse miembros del público¹⁰². En otro caso, Muhammad Jibril Abdul Rahman, también conocido como Muhammad Ricky Ardan (el “Príncipe de la Yihad”), fue condenado a cinco años de prisión por complicidad en un acto de terrorismo.

134. En Singapur, en el contexto de Internet, el artículo 4 2 g) del Código de Prácticas de Internet de Singapur prohíbe la difusión de materiales que “glorifiquen, fomenten o aprueben el odio, la discordia o la intolerancia por motivos raciales, étnicos o religiosos”.

2. El estado de derecho y la penalización de la incitación

135. Cuando insta a los Estados a tipificar la incitación a la comisión de actos terroristas, la resolución 1624 (2005) del Consejo de Seguridad establece expresamente que los Estados deben asegurarse de que las medidas que adopten para aplicar lo dispuesto en la resolución se ajusten a las obligaciones que les incumben en virtud del derecho internacional, en particular las normas jurídicas de derechos humanos, el derecho relativo a los refugiados y el derecho humanitario.

136. Este principio, que también se refleja en los instrumentos universales contra el terrorismo, se ha reafirmado muchas veces a nivel internacional (incluso en el marco de las Naciones Unidas), es un elemento fundamental del enfoque de “estado de derecho” de la UNODC para el fortalecimiento de las respuestas de la justicia penal al terrorismo en el marco del régimen jurídico universal contra el terrorismo y ha sido reafirmado en muchos instrumentos regionales contra el terrorismo y de derechos humanos, en particular los elaborados por el Consejo de Europa, que ya se mencionaron (véase la sección II. D *supra*)¹⁰³.

137. No es posible, dentro de los límites de la presente publicación, analizar a fondo, en el marco del respeto de los derechos humanos garantizados a la libertad de expresión, todos los comentarios y fuentes de jurisprudencia disponibles sobre el alcance preciso y la aplicación correcta de las disposiciones legales adoptadas por los países para penalizar la incitación a la comisión de actos terroristas.

¹⁰² Véase www.indonesiamatters.com/624/wwwansharnet-chatroom-jihad.

¹⁰³ Véanse los informes del Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo al Consejo de Derechos Humanos y a la Asamblea General, en los que el Relator Especial expresó su preocupación por el posible efecto que la legislación contra la incitación podría tener sobre la libertad de palabra y expresión, al promover la penalización de la libertad de expresión que no alcanza a ser incitación al terrorismo. Estas opiniones e inquietudes se pusieron de relieve en una comunicación escrita presentada a la reunión del grupo de expertos por la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos; véase también la Declaración conjunta sobre libertad de expresión e Internet, formulada el 1 de junio de 2011 por el Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, el Representante para la Libertad de los Medios de Comunicación de la Organización para la Seguridad y la Cooperación en Europa, la Relatora Especial para la Libertad de Expresión de la Organización de los Estados Americanos y la Relatora Especial para la libertad de expresión y el acceso a la información en África de la Comisión Africana de Derechos Humanos y de los Pueblos, en las que reafirmaron la importancia fundamental del derecho a la libertad de expresión.

138. No obstante, aunque la doctrina legal existente sobre el alcance preciso de los instrumentos internacionales de derechos humanos, tales como el artículo 10, párrafo 1, del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales y el artículo 19 del Pacto Internacional de Derechos Civiles y Políticos deja margen para el debate en curso, está claro que, en la práctica, encontrar el equilibrio justo entre la protección del derecho a la libertad de expresión y la aplicación de la legislación penal dirigida a combatir la incitación a la comisión de actos terroristas sigue siendo un reto para los gobiernos.

3. *Facultades de las fuerzas del orden*

139. La investigación de los casos de terrorismo con uso de Internet u otros servicios conexos por presuntos terroristas suele exigir la realización de actividades intrusivas o coercitivas de registro, vigilancia o monitorización por los servicios de inteligencia o los organismos encargados de hacer cumplir la ley. Es importante para el éxito de cualquier proceso judicial, por tanto, que estas técnicas de investigación estén debidamente autorizadas por las leyes nacionales y, como siempre, que la legislación de apoyo defienda los derechos humanos fundamentales protegidos por las normas jurídicas internacionales de derechos humanos.

a) Facultades de registro, vigilancia e interceptación

140. En Israel, la cuestión de las facultades de investigación para la obtención de pruebas digitales en Internet se trata, respecto tanto de los delitos en general como de los relacionados con el terrorismo en particular, en la Ley de computadoras de 1995, que define ciertas facultades específicas para la obtención de pruebas digitales. La Ley de computadoras modificó la Ley de escuchas telefónicas, por estimarse que la captación de comunicaciones entre computadoras equivalía a una “escucha telefónica” y, por tanto, permitía a las autoridades investigadoras obtener autorización judicial o administrativa en casos excepcionales y urgentes, para captar los datos transferidos en la comunicación entre computadoras.

141. En 2007, se promulgó la Ley de datos sobre comunicaciones. El propósito de esa ley era organizar, de manera más estructurada y progresiva, la práctica establecida en cuanto a la obtención de datos sin contenido (datos de tráfico) de las empresas de telefonía fija y móvil, así como de los proveedores de acceso a Internet. La Ley no se aplica a los proveedores de servicios de Internet, que ofrecen otros servicios, como el almacenamiento de información, intercambio de información, correo electrónico, servicios sociales y demás. En la actualidad, en los casos en que las autoridades desean obtener información de los proveedores de servicios de Internet, es aplicable una disposición legal anterior que les permite, en general, emitir una citación con apercibimiento y obtener información de cualquier persona que tenga información que pueda ser de utilidad para la investigación.

142. En 2010, el Gobierno de Israel promovió un proyecto de ley para la codificación de las facultades de investigación en relación con los datos tanto físicos como digitales. El proyecto de ley tiene por objeto organizar, de manera avanzada, la reunión de

pruebas digitales. Contiene una estructura ordenada de facultades que actualmente no están previstas en la legislación israelí, tales como los registros secretos de computadoras (en el caso de delitos especialmente graves), la obtención de información para ser almacenada (en el futuro) en una computadora especial, la manera en que se han de obtener los mensajes de correo electrónico en poder del proveedor del servicio, y el registro de material informático con autorización administrativa en ciertas circunstancias. De aprobarse, estas medidas se aplicarían a los casos de terrorismo relacionados con el uso de Internet.

143. En 2006, el Gobierno de Francia aprobó nueva legislación contra el terrorismo que facilita, a los efectos de las investigaciones relacionadas con el terrorismo, la vigilancia de las comunicaciones y el acceso de la policía a los datos de comunicaciones de las compañías telefónicas, los proveedores de servicios de Internet y los cibercafés.

144. La Ley de lucha contra el terrorismo y sobre diversas normas de seguridad y de control de las fronteras (2006-64, de 23 de enero de 2006) dispone que los proveedores de servicios de Internet, los cibercafés, los proveedores de hospedaje y las compañías telefónicas deben comunicar los datos de tráfico, los números llamados y las direcciones IP a los organismos gubernamentales especializados en casos relacionados con la investigación de presuntas actividades terroristas.

145. En virtud del artículo 6, las compañías de telefonía móvil y los cibercafés están obligados a llevar un registro de las conexiones de clientes durante 12 meses y ponerlo a disposición de la policía. La ley también autoriza el uso de cámaras de vigilancia en los espacios públicos, como estaciones de tren, iglesias y mezquitas, tiendas, fábricas y centrales nucleares. El artículo 8 autoriza a la policía a monitorizar automáticamente los vehículos y sus ocupantes en las carreteras y autopistas francesas (sacando, incluso, fotografías de las matrículas de los vehículos y de los ocupantes) y a monitorizar a los concurrentes en grandes reuniones públicas¹⁰⁴.

146. En fecha más reciente, el 14 de marzo de 2011, se modificó el Código de Procedimiento Penal para otorgar facultades adicionales a las autoridades encargadas de las investigaciones de atentados terroristas. Estas enmiendas incluyen la facultad para incautarse de los documentos pertinentes para una investigación (incluidas la conversión y la transferencia de datos de computadora), y permiten el descifrado de datos informáticos protegidos, la infiltración digital, la captura de datos informáticos (incluidas las imágenes), las escuchas telefónicas y la interceptación de otras comunicaciones. Además, la ley establece la base jurídica para las actividades de los funcionarios policiales que participan, entre otras cosas, en las discusiones en línea de las salas de charla, como parte de las investigaciones de delitos relacionados con la incitación al terrorismo. Este es un tema jurídico importante que los gobiernos tal vez deseen considerar. Estas disposiciones proporcionan a los servicios franceses encargados de hacer cumplir la ley la posibilidad, entre otras cosas, de obtener pruebas relacionadas con los datos de conexión de los mensajes electrónicos, las comunicaciones telefónicas y las direcciones IP.

¹⁰⁴www.edri.org/edriagram/number4.2/frenchlaw.

147. El experto de China se refirió a los reglamentos de ese país que facultan a la policía, cuando investiga un delito en que se hizo uso de Internet, para ordenar al proveedor de servicios de Internet y al proveedor de comunicaciones por Internet que entreguen los documentos y datos pertinentes, que están obligados a retener por ley durante 60 días.

148. En el Reino Unido, la Ley de reglamentación de los poderes de investigación de 2000 establece un marco jurídico que regula los cinco siguientes tipos de actividades de vigilancia realizadas por los organismos gubernamentales:

- Interceptación de comunicaciones (por ejemplo, interceptación de llamadas telefónicas o acceso al contenido de mensajes electrónicos)
- Vigilancia intrusiva (por ejemplo, vigilancia encubierta en locales privados o vehículos)
- Vigilancia dirigida (por ejemplo, vigilancia secreta de un blanco identificado en un lugar público)
- Fuentes humanas de inteligencia secretas (por ejemplo, agentes encubiertos)
- Datos sobre comunicaciones (por ejemplo, registros relacionados con las comunicaciones, pero no el contenido de tales comunicaciones)¹⁰⁵.

149. Además de establecer para qué fines y por qué procedimientos se han de autorizar dichas actividades, la Ley obliga a las autoridades encargadas de la vigilancia a determinar si el ejercicio de estas facultades y la injerencia en los derechos de las personas vigiladas son proporcionados, así como a adoptar medidas para evitar lo que se conoce como “intrusión colateral”, en que se ven afectados los derechos de terceros que no están sometidos a vigilancia. En el caso de que las comunicaciones objeto de investigación estén cifradas, la Ley también tipifica como delito el acto, por parte de quienes tengan en su poder las claves correspondientes, de no revelarlas a los investigadores autorizados¹⁰⁶.

150. En el año 2000, el Gobierno de la India aprobó la Ley de Tecnología de la Información 2000, que se modificó en 2008, para establecer el delito de “terrorismo cibernético” (artículo 66F) y abordar otras cuestiones relacionadas con Internet. El artículo 67C 1) de la Ley trata de la retención de los datos y dispone que los proveedores regulados “deberán conservar y retener la información que pueda especificarse por el tiempo y en la forma y formato que prescriba el Gobierno central” y tipifica como delito (castigado con hasta tres años de prisión y multas) el contravenir a sabiendas esa obligación.

151. El artículo 69 1) de la Ley faculta a las autoridades gubernamentales para dictar instrucciones de “interceptación, monitorización y descifrado de la información

¹⁰⁵“Summary of surveillance powers under the Regulation of Investigatory Powers Act”, National Council for Civil Liberties.

¹⁰⁶Ian Walden, *Computer Crimes and Digital Investigations* (Oxford University Press, 2007), pág. 216.

generada, transmitida, recibida o almacenada en cualquier dispositivo informático” y establece las obligaciones y garantías jurídicas que deben acompañar a dichos actos estatales, mientras que el artículo 69A 1) faculta a los organismos del Estado para dictar instrucciones de bloqueo del acceso del público por medios informáticos a toda información cuya supresión sea, a juicio de esos organismos, necesaria o conveniente, en aras de la soberanía, la integridad, la seguridad y las relaciones internacionales de la India, o para impedir la incitación a la comisión de delitos conexos “de competencia de un tribunal”, incluido el terrorismo. Finalmente, el artículo 69B faculta a determinados organismos del Estado para monitorizar, reunir y almacenar datos de tráfico o la información generada, transmitida o recibida a través de cualquier dispositivo informático.

152. En Nueva Zelanda, la Ley de registro y vigilancia de 2012 actualiza, consolida y armoniza las facultades de los organismos encargados de hacer cumplir la ley para registrar, vigilar e interceptar comunicaciones a fin de hacer frente a las nuevas formas de tecnología. La Ley crea una nueva definición de la expresión “registros de sistemas informáticos”, que se hace extensiva al registro de computadoras que no están conectadas internamente, pero son capaces de acceder a una red a distancia.

153. Con el fin de reforzar las garantías jurídicas, la Ley deja claro que el registro de computadoras de acceso remoto está permitido solo en dos situaciones: cuando una computadora tiene la capacidad de acceder legalmente a un sistema informático objeto del registro y, por tanto, es considerada parte de ese sistema; y cuando no hay ningún lugar físico que registrar (por ejemplo, en el caso del correo electrónico, al que el usuario puede acceder desde distintos lugares, como los cibercafés). La Ley también establece que cuando la policía practique registros autorizados de servicios de datos de Internet de acceso remoto, deberá dirigir una notificación del registro por correo electrónico, remitida a la dirección electrónica del servicio objeto del registro.

b) Cuestiones asociadas a la facultad de interceptación

154. Cuando las autoridades emprenden actividades de monitorización, vigilancia o interceptación de las comunicaciones electrónicas, necesitan la cooperación de los proveedores de servicios públicos de telecomunicaciones o servicios conexos. Aunque en muchos casos las compañías privadas están dispuestas a prestar asistencia a los organismos policiales que actúan en ejercicio de sus funciones legales, está claro que hay límites en cuanto al tiempo y los recursos que estarán dispuestos a dedicar a título totalmente gratuito. Por tanto, convendría que los gobiernos proporcionasen una base jurídica clara para las obligaciones que han de imponerse a las entidades del sector privado, incluidas las especificaciones técnicas exigidas a sus redes y la forma de sufragar el costo de esos servicios.

155. En Israel, el artículo 13 de la Ley de Comunicaciones de 1982 establece que el Primer Ministro podrá ordenar a los proveedores de acceso a Internet, dentro de Israel, que introduzcan las modificaciones tecnológicas que requieran las fuerzas de seguridad (que, según se definen, incluyen los servicios de policía, de seguridad y otros servicios especiales) para los fines de la lucha contra el terrorismo. La Ley se aplica solo a los

proveedores de acceso a Internet, que, con arreglo a las leyes israelíes, reciben sus licencias del Ministerio de Comunicaciones. No se aplica a los proveedores de servicios de almacenamiento de datos o de servicios de gestión de contenido que operan en Israel, ya que estos proveedores no necesitan licencia del Ministerio.

156. En Nueva Zelanda, la Ley de telecomunicaciones (capacidad de interceptación) de 2004 precisa las obligaciones de los operadores de redes de asistir a los organismos oficiales autorizados en la ejecución de operaciones de interceptación o la entrega autorizada de datos asociados a llamadas. La Ley obliga a los operadores de red a garantizar que todas las redes públicas de telecomunicaciones o de servicios que poseen, controlan o mantienen en funcionamiento tengan capacidad de interceptación. Se considera que las redes o los servicios tienen esta capacidad cuando los organismos oficiales autorizados pueden interceptar las telecomunicaciones o los servicios de manera tal que se identifiquen e intercepten solo las telecomunicaciones objeto de investigación, se suministren los datos asociados a llamadas y los contenidos de estas (en una forma utilizable) y permitan una interceptación discreta, oportuna y eficiente de manera que proteja la privacidad de otros usuarios de las telecomunicaciones y evite una injerencia indebida. La Ley también obliga a los operadores de red a proporcionar los medios para descifrar cualquier telecomunicación transmitida por su red si el contenido está cifrado y el operador de la red ha proporcionado los medios de cifrado.

157. Reconociendo el tiempo y el costo que supone para algunos operadores de red cumplir con estos requisitos, la Ley concede a los operadores afectados un plazo que va de 18 meses a cinco años (según el estado de la red) para adquirir esta capacidad. Por otra parte, el Gobierno ha accedido a sufragar los gastos de la adquisición de capacidad de interceptación en las redes que ya estaban en funcionamiento en la fecha de promulgación de la Ley y carecían de la capacidad de interceptación necesaria.

158. En el Brasil, la Ley Federal núm. 9.296 de 1996, junto con el artículo 5 (XII) de la Constitución Federal de 1988, regula las escuchas telefónicas por los organismos oficiales autorizados. Si bien reconoce que es inviolable el secreto de las telecomunicaciones, la Ley prevé, con sujeción a una orden judicial, casos específicos de suspensión de este principio para fines de investigación criminal o instrucción penal. La Ley establece los procedimientos que han de seguirse en casos de escuchas telefónicas, que se realizan bajo la supervisión de un juez. Una vez ejecutada la intervención telefónica, se transcriben los resultados, que se entregan al juez, junto con un resumen de todas las medidas adoptadas en virtud de la autorización (artículo 6).

159. A fin de cumplir con sus obligaciones legales, las empresas de telecomunicaciones se han visto obligadas a establecer y capacitar unidades especializadas e invertir en la tecnología necesaria. En cuanto al costo de adquirir capacidad de interceptación, corresponde a las empresas de telecomunicaciones proporcionar el personal y los recursos técnicos necesarios para prestar apoyo a las actividades autorizadas de interceptación. Este enfoque refleja el hecho de que, con arreglo a la Constitución del Brasil, las empresas brasileñas de telecomunicaciones operan en virtud de una concesión del Gobierno y se considera que los servicios de telecomunicaciones son un servicio público.

160. En Indonesia, a raíz de los atentados de Bali de 2002, el Gobierno aprobó legislación antiterrorista que permite a los organismos de aplicación de la ley y de seguridad, a los efectos de las investigaciones relacionadas con el terrorismo, interceptar y examinar la información que se expresa, envía, recibe o archiva por medios electrónicos o con un dispositivo óptico. En relación con el período de retención de ficheros de Internet o de registro, esta cuestión está regulada por la Ley núm. 11 de 2008 sobre la información y las operaciones electrónicas, concretamente el artículo 6, párrafo 1, apartado a, que obliga a cada sistema operado por un proveedor de sistemas electrónicos a reproducir en forma completa cualquier información electrónica y/o documento electrónico durante todo el período de retención que manda la ley.

161. En Argelia, en 2006, el Gobierno aprobó una ley que permite la vigilancia de video y micrófono y la interceptación de correspondencia, si están autorizadas y se ejecutan bajo supervisión directa del fiscal. La misma ley autoriza la técnica de infiltración con el fin de investigar el terrorismo o la delincuencia organizada y permite que el agente cometa, en el curso de la infiltración, infracciones leves especificadas. El secreto de la identidad del agente está cuidadosamente protegido por la ley, pero la infiltración debe llevarse a cabo bajo la autoridad del fiscal o del juez de instrucción¹⁰⁷.

162. En Malasia, la Ley de las Comunicaciones y Multimedia de 1998 contiene varias disposiciones relativas a la regulación de las investigaciones de Internet e investigaciones penales conexas. Por ejemplo, el artículo 249 de la Ley, que trata de la cuestión del acceso a los datos informáticos durante los registros, establece que el acceso incluye la obtención de “contraseñas, claves de cifrado o descifrado, software o equipo y demás medios necesarios para permitir la comprensión de los datos informáticos”.

163. Además, el capítulo 4 de la Ley, relativo a asuntos de interés nacional, impone una obligación general a los operadores de servicios de Internet de obrar “con el mayor empeño” para garantizar que los servicios de la red no se utilicen para la comisión de ninguno de los delitos previstos en el derecho de Malasia (artículo 263) y establece que el ministro responsable podrá ordenar, especificando los requisitos técnicos del caso, que un licenciatario o categoría de licenciatarios adquiera o adquieran la capacidad de permitir la interceptación autorizada de las comunicaciones (artículo 265).

164. El capítulo 2 de la Ley se refiere a la cuestión del contenido ofensivo y prohíbe a los proveedores de servicios de aplicaciones de contenido y a todas las personas que utilizan esos servicios proporcionar contenido alguno que sea “indecente, obsceno, falso, amenazador, o de carácter ofensivo, y se haga con la intención de molestar, abusar, amenazar o acosar a cualquier otra persona” (artículo 211). Aquel que infrinja estas obligaciones cometerá un delito y será reprimido con una multa no superior a 50.000 ringgit (unos 16.200 dólares de los Estados Unidos) o con una pena de prisión por un término no superior a un año, o ambas cosas, y también podrá ser objeto de una sanción permanente de 1.000 ringgit (aproximadamente 325 dólares de los Estados

¹⁰⁷ Oficina de las Naciones Unidas contra la Droga y el Delito, *Compendio de casos relativos a la lucha contra el terrorismo*, párr. 215.

Unidos) por cada día o parte de un día durante el cual el delito continúe después de la condena. El artículo 212 de la Ley prevé la designación de un organismo del sector para desempeñarse como foro con el fin de elaborar un código del sector en materia de contenidos.

165. En los Estados Unidos, los operadores de telecomunicaciones están obligados actualmente, en virtud de la Ley de asistencia de las [empresas de] comunicaciones a las fuerzas del orden de 1994, a proporcionar capacidad de interceptación en las redes de telefonía y banda ancha.

c) Regulación de los cibercafés

166. Se sabe que los terroristas se han servido de cibercafés, en algunos casos, para llevar a cabo actos relacionados con el terrorismo; sin embargo, no hay datos sobre la proporción de este tipo de actividad en relación con las actividades legítimas realizadas a través de estos servicios de Internet.

167. La cuestión de la medida en que los gobiernos deberían, para combatir el terrorismo, regular Internet o los cibercafés es un tema complejo, muy ligado a cuestiones de derechos humanos. A nivel internacional, existen distintos enfoques. En algunos Estados, como Egipto, la India, Jordania y el Pakistán, los Gobiernos aplican medidas legislativas o reglamentarias concretas que obligan a los operadores de cibercafés a obtener, retener y, previa solicitud, entregar una identificación con fotografía, domicilio y datos de uso y conexión de los clientes a los organismos encargados de hacer cumplir la ley.

168. Si bien los gobiernos pueden imponer obligaciones a los operadores de cibercafés encaminadas a restringir el uso indebido de esos servicios por terroristas, la utilidad de esas medidas es cuestionable, sobre todo cuando hay otros servicios de Internet a disposición del público (por ejemplo, las computadoras de las bibliotecas públicas o locales públicos con conexión inalámbrica a Internet (Wi-Fi)) que ofrecen oportunidades similares para el uso anónimo de Internet por terroristas. Cabe señalar que en 2005, el Gobierno de Italia impuso obligaciones reglamentarias a los operadores de los cibercafés respecto de la identificación de los clientes; sin embargo, esta reglamentación fue abolida a finales de 2010, en parte, por el temor al efecto que podría tener este tipo de reglamentación en el desarrollo de los servicios de Internet y a la reacción de los usuarios legítimos.

d) Control del contenido

169. La cuestión de la medida en que los gobiernos deben regular los contenidos relacionados con el terrorismo en Internet es muy discutible. Los enfoques varían considerablemente, y en tanto que algunos Estados aplican a Internet y a otros proveedores de servicios conexos estrictos controles reglamentarios, recurriendo incluso en ciertos casos al uso de tecnología para filtrar o bloquear el acceso a algunos contenidos, otros adoptan un enfoque reglamentario más liberal, confiando en mayor medida en la autorregulación del sector de la información.

170. En el artículo “Terrorism and the Internet: should web sites that promote terrorism be shut down?” (El terrorismo e Internet: ¿deberían cerrarse los sitios web que promueven el terrorismo?)¹⁰⁸, Barbara Mantel observa que “la mayoría de los proveedores de servicios de Internet, empresas de hospedaje de sitios web, de intercambio de ficheros y de redes sociales tienen acuerdos de condiciones de servicio que prohíben determinados contenidos”. Por ejemplo, señala, el servicio de hospedaje de sitios web para pequeñas empresas comerciales, de Yahoo, prohíbe expresamente que los usuarios utilicen el servicio para proporcionar apoyo o recursos materiales a cualquier organización u organizaciones designadas por el Gobierno de los Estados Unidos como una organización terrorista extranjera. En ese sentido, hay cierta medida de autorregulación en la sociedad de la información.

171. Al evaluar el enfoque y el nivel de intervención en esta esfera, los gobiernos deben tener en cuenta una serie de factores, incluidos el lugar donde se hospeda el contenido, las garantías constitucionales o de otra índole relacionadas con el derecho a la libertad de expresión, el contenido mismo y las consecuencias estratégicas, desde el punto de vista de los servicios de inteligencia o de aplicación de la ley, de monitorizar ciertos sitios o de infiltrarse en ellos o de hacerlos inaccesibles¹⁰⁹.

172. En el Reino Unido, el artículo 3 de la Ley de Terrorismo de 2006 contiene un recurso innovador, a disposición de las autoridades que se ocupan de los casos de posibles actos de incitación por Internet, que faculta a la policía para emitir una notificación de retiro (“take down” notice) a las personas asociadas con el funcionamiento de sitios web o con otros contenidos de Internet.

173. El artículo 3 de la Ley se aplica a los casos de delitos tipificados en los artículos 1 y 2 de esa Ley en que “a) se publica, o se hace publicar, una declaración en el curso de, o en conexión con, la prestación o el uso de un servicio prestado por vía electrónica, o b) se realizan actos comprendidos dentro del ámbito de aplicación del artículo 2 2) [difusión de una publicación terrorista] en el curso de, o en conexión con, la prestación o el uso de dicho servicio”.

174. El artículo 3 2) establece que si la persona a la que se ha hecho la notificación no retira el contenido relacionado con el terrorismo, y si es posteriormente acusada de delitos en virtud de los artículos 1 o 2 de la Ley de Terrorismo de 2006 en relación con dicho incumplimiento, se podrá hacer en el juicio una presunción *juris tantum* de que el contenido en cuestión tenía su aprobación.

175. A pesar de la disponibilidad de estas notificaciones de retiro como medida preventiva, en la práctica esta facultad no se ha usado todavía. En la mayoría de los casos, especialmente cuando el contenido ofensivo está hospedado en sitios web de terceros, tiende a contravenir los términos y condiciones de servicio del proveedor, de modo que

¹⁰⁸Barbara Mantel, “Terrorism and the Internet: should web sites that promote terrorism be shut down?”, *CQ Global Researcher*, vol. 3, núm. 11 (noviembre de 2009).

¹⁰⁹Catherine A. Theohary y John Rollins, “Terrorist use of the Internet: information operations in cyberspace”, Congressional Research Service report (8 de marzo de 2011), pág. 8.

las autoridades pueden negociar con éxito la eliminación del contenido prohibido. De hecho, en el Reino Unido, la unidad especializada en derivaciones, en la lucha contra el uso de Internet por terroristas, coordina las respuestas nacionales a las denuncias del público, así como del Gobierno y del sector de las comunicaciones, de contenidos de Internet relacionados con el terrorismo y actúa como centro especial de asesoramiento de la policía.

4. *Cooperación internacional*

176. Los Estados están obligados, en virtud de varios instrumentos internacionales, regionales, multilaterales y bilaterales relacionados con el terrorismo y la delincuencia organizada transnacional, a establecer políticas y marcos legislativos para facilitar la cooperación internacional eficaz en la investigación y persecución de este tipo de casos.

177. Además de contar con políticas y leyes con las figuras delictivas necesarias para satisfacer los requisitos de la doble incriminación, los Estados deben promulgar una legislación amplia que ofrezca a las autoridades una base jurídica para la cooperación internacional con sus homólogos extranjeros en las investigaciones relacionadas con el terrorismo transnacional. En los casos en que se ha usado Internet, es muy probable que una cooperación internacional eficaz, incluida la capacidad de compartir información y, en particular, los datos relacionados con Internet, sea un factor clave para el éxito de cualquier proceso penal.

178. Las cuestiones relacionadas con la cooperación internacional en los casos de terrorismo se tratan con mayor detalle en el capítulo V *infra*.

IV. Investigaciones y reunión de inteligencia

A. Recursos que ofrece Internet para la comisión de delitos terroristas

179. Los avances tecnológicos han proporcionado a los terroristas muchos medios sofisticados que les permiten servirse de Internet con fines ilícitos. Las investigaciones eficaces de las actividades en Internet se basan en una combinación de métodos de investigación tradicionales, el conocimiento de los instrumentos disponibles para llevar a cabo actividades ilícitas por Internet y el desarrollo de prácticas dirigidas a descubrir, detener y procesar a los autores de esos actos.

180. Un caso de Francia ilustra cómo se emplean simultáneamente diferentes tipos de técnicas de investigación, tanto las tradicionales como las ideadas específicamente en relación con las pruebas digitales, a fin de reunir los elementos de prueba necesarios para procesar con éxito a los terroristas que usan Internet.

Ministerio público c. Arnaud, Badache, Guihal y otros

En esta causa francesa hay varios implicados: Rany Arnaud, Nadir Zahir Badache, Adrien Luciano Guihal y Youssef Laabar, que fueron sentenciados el 26 de enero de 2012 por el Tribunal Correccional de París y condenados a penas de prisión que van desde los 18 meses hasta los 6 años por, entre otras cosas, difundir material relacionado con el terrorismo.

Arnaud, Badache y Guihal fueron detenidos en Francia en diciembre de 2008 después de que Arnaud, que operaba con el nombre de usuario de "Abdallah", publicara mensajes que llamaban a la yihad contra Francia en un sitio web de propaganda, minbar-sos.com:

"No te olvides de que Francia sigue luchando contra nuestros hermanos en el Afganistán y tú estás en un país en guerra; apresúrate a buscar el martirio cuanto antes; boicotea su economía, derrocha sus riquezas, no apoyes su economía y no contribuyas a la financiación de sus ejércitos".

Como resultado de la publicación, las autoridades interceptaron la cuenta de Arnaud en Internet, lo pusieron bajo vigilancia física e intervinieron su línea telefónica. Después de detener a Arnaud, los investigadores hicieron un examen forense del contenido de las computadoras que utilizaba y descubrieron que había buscado información sobre cuestiones relacionadas con la comisión de actos terroristas; por ejemplo, sobre productos que podían utilizarse para fabricar explosivos y artefactos incendiarios y sobre posibles blancos; había seguido, además, las actividades de una empresa que usaba nitrato de amonio. Las investigaciones revelaron que Arnaud había reclutado a Guihal y Badache, participado en reuniones y discusiones para preparar un atentado, establecido contacto con participantes en movimientos yihadistas buscando ayuda para ejecutar sus planes y recibido remesas para su financiación. Estos actos son todos delitos de conformidad con los artículos 421-2-1, 421-1, 421-5, 422-3, 422-6 y 422-7 del Código Penal francés, y los artículos 203 y 706-16 y ss. del Código de Procedimiento Penal.

El Tribunal consideró que el plan en que Arnaud, supuestamente, había tomado parte en asociación con los otros delincuentes, consistente en la colocación de explosivos en un camión que explotaría al llegar a destino, representaba una amenaza particularmente grave al orden público. Por consiguiente, Arnaud fue condenado a seis meses de prisión por cargos relacionados con la participación en un grupo formado para cometer actos delictivos con el fin de preparar un atentado terrorista; posesión de varios documentos fraudulentos, y uso fraudulento de documentos administrativos que acreditaban un derecho, una identidad o una calidad o la concesión de una autorización. Por ese mismo cargo, Badache fue condenado a dos años de prisión, con seis meses en suspenso, mientras que Guihal fue condenado a cuatro años, con un año en suspenso. Laabar, a quien se acusaba de otros delitos conexos, fue condenado a 18 meses de prisión.

181. La investigación y persecución de los casos fundamentados en pruebas digitales exigen estar familiarizado con las técnicas especializadas de investigación penal y tener la formación, los conocimientos y la experiencia adecuados para aplicar esas técnicas en un entorno virtual. Si bien la admisibilidad de las pruebas es en última instancia una cuestión de derecho y es, por tanto, de competencia del fiscal, los investigadores deben estar familiarizados con los requisitos legales y de procedimiento para establecer la admisibilidad a efectos de investigaciones tanto nacionales como internacionales. Si se quiere lograr el éxito de una causa, es necesario contar con el apoyo de investigadores dotados de un sólido conocimiento práctico de los requisitos de las normas probatorias aplicables, sobre todo con respecto a las pruebas digitales, pues ello facilita la obtención de suficientes pruebas admisibles. Por ejemplo, los procedimientos utilizados en la reunión, la conservación y el análisis de pruebas digitales deben garantizar que se mantenga una clara “cadena de custodia”, desde el momento en que se obtienen por primera vez, de manera que no puedan haber sido objeto de manipulaciones desde el momento de su incautación hasta su producción final en juicio¹¹⁰.

1. Comunicaciones basadas en Internet

a) Telefonía de voz por Internet

182. Durante la última década, las aplicaciones que permiten a los usuarios comunicarse en tiempo real utilizando la telefonía de voz por Internet (VoIP) y charlas con video o de texto han crecido en popularidad y sofisticación. Algunas de estas aplicaciones ofrecen funciones avanzadas de intercambio de información que permiten a los usuarios, por ejemplo, compartir ficheros o ver a distancia la actividad en pantalla de otro usuario en tiempo real. La telefonía VoIP, en particular, se usa cada vez más por su utilidad para comunicarse por Internet. Entre los proveedores de servicios VoIP más conocidos cabe mencionar a Skype y Vonage, que operan mediante la conversión de sonido analógico a formato digital comprimido, lo cual permite la transferencia de paquetes digitales de información a través de Internet, utilizando conexiones de ancho de banda relativamente reducido.

183. Como la telefonía VoIP consiste en la transmisión de paquetes de datos digitales, en lugar de señales analógicas, y los proveedores de servicios suelen generar facturas para los abonados relacionadas con el uso de Internet en función del volumen de datos global, las llamadas VoIP de computadora a computadora no se facturan sobre la base de cada llamada, como se hace con las llamadas tradicionales de telefonía móvil y de línea fija. Esta diferencia en las prácticas de facturación puede tener un efecto importante en las investigaciones relacionadas con las comunicaciones VoIP, ya que hace que sea más difícil para las autoridades encargadas de hacer cumplir la ley corroborar dichas comunicaciones con los marcadores correspondientes, por ejemplo, la hora de la llamada y la ubicación de los participantes. Otros indicadores, empero, como la oportunidad y el volumen de tráfico de datos de Internet, también pueden proporcionar un medio para identificar a los autores de actividades ilícitas en Internet (véase el párr. 205 *infra*). Además, si bien el origen y destino de las llamadas telefónicas convencionales pueden encaminarse a través de interruptores de línea fija o torres de comunicación celular, que dejan huellas de ubicación geográfica, las comunicaciones VoIP basadas totalmente en Internet, a través por ejemplo de redes inalámbricas, pueden plantear dificultades a la investigación. Otros factores que complican los problemas derivados del uso de la tecnología VoIP pueden estar relacionados, entre otras cosas, con el encaminamiento de las llamadas a través de redes P2P y el cifrado de los datos de llamada (que se examinan con más detalle en la sección IV. A. 2 *infra*)¹¹¹.

184. Las solicitudes de información presentadas debidamente a los proveedores de servicios VoIP pueden, no obstante, proporcionar información valiosa para los fines de la identificación, como la dirección IP, la dirección electrónica o los datos de pago de un usuario.

b) *Correo electrónico*

185. Los servicios de correo electrónico basados en la web también ofrecen a los terroristas un medio encubierto de comunicación, que puede ser usado indebidamente para fines ilícitos. Los mensajes de correo electrónico enviados entre las partes por lo general contienen una serie de elementos que pueden ser útiles para el investigador. Un mensaje electrónico típico puede constar del encabezado del sobre, el encabezado del mensaje, el cuerpo del mensaje y ficheros adjuntos. Si bien es posible que solo aparezca una versión abreviada del encabezado del sobre, según los ajustes del software de la aplicación, el encabezado completo del sobre generalmente contiene una constancia de cada uno de los servidores por los cuales pasó el mensaje en camino hacia el destinatario final, así como información relativa a la dirección IP del remitente¹¹². La información contenida en el encabezado del sobre es menos susceptible a la manipulación (aunque no es invulnerable) que el encabezado del mensaje, que generalmente consiste en información proporcionada por el usuario en campos tales como “Para”, “De”, “Trayecto de retorno”, “Fecha” y “Hora”, como aparece en el dispositivo desde el que se envió el mensaje¹¹³.

¹¹¹Comunicación escrita del experto del Raggruppamento Operativo Speciale de los Carabinieri de Italia.

¹¹²Estados Unidos, Departamento de Justicia, Oficina de Programas Judiciales, Instituto Nacional de Justicia, *Investigations Involving the Internet and Computer Networks* (2007), pág. 18 y ss.

¹¹³Ibid., pág. 20.

186. Una técnica muy utilizada para reducir los rastros electrónicos entre las partes, y por tanto la probabilidad de detección, es la comunicación a través de mensajes no enviados, guardados en la carpeta de borradores de la cuenta de correo electrónico. Esta información está a disposición de múltiples destinatarios que usan una contraseña compartida para acceder a la cuenta. Pueden tomarse otras medidas para evitar la detección, por ejemplo el uso de una terminal de acceso público a distancia, como un cibercafé, para acceder al borrador. Este método fue utilizado en los atentados terroristas de Madrid de 2004.

187. También es posible emplear técnicas de anonimato (que se discuten en mayor detalle en la sección IV. A. 2, *infra*) en relación con las comunicaciones de correo electrónico, por ejemplo ocultando la dirección IP asociada con el remitente de un mensaje electrónico. También se pueden usar servidores de correo que preservan el anonimato, eliminando la información de identificación del encabezado del sobre antes de enviarlo al servidor de correo siguiente.

Importancia de la cooperación internacional en la investigación de actividades relacionadas con el terrorismo realizadas por Internet

El experto del Raggruppamento Operativo Speciale (Grupo de Operaciones Especiales) de los Carabinieri de Italia reseñó el papel fundamental de la cooperación internacional y de las técnicas de investigación especializadas en la investigación del uso de Internet con fines terroristas por la organización extremista basada en Turquía, el Frente del Partido Revolucionario de Liberación Popular (DHKP-C). La estrecha colaboración entre los funcionarios encargados de hacer cumplir la ley de Turquía e Italia permitió a los investigadores italianos descubrir las técnicas de cifrado y otras medidas de seguridad de los datos utilizadas por los miembros del DHKP-C para intercambiar información con fines de promoción del terrorismo, entre otros, a través de los servicios de correo en línea. En particular, los miembros del DHKP-C empleaban el software de esteganografía Camouflage para ocultar datos dentro de imágenes en formato JPEG y GIF, y software de WinZip para cifrar ficheros, que se remitían adjuntos a las comunicaciones por correo electrónico (véase la sección IV. A. 2 *infra*). Los investigadores italianos interceptaron u obtuvieron contraseñas de cifrado por otros medios y reconocieron los programas pertinentes para ayudar a descifrar las comunicaciones. Se obtuvo información adicional mediante el análisis informático forense, con software EnCase (véase la sección IV. C *infra*) y las técnicas tradicionales de investigación, para permitir a los investigadores obtener pruebas digitales de las computadoras de un sospechoso al que estaban investigando. Los resultados de esta investigación, junto con una estrecha cooperación transfronteriza, condujeron a la detención, en abril de 2004, de 82 sospechosos en Turquía y de otros 59 sospechosos en Alemania, Bélgica, Grecia, Italia y los Países Bajos.

c) *Servicios de mensajería en línea y salas de charla*

188. Los servicios de mensajería en línea y las salas de charla proporcionan medios adicionales de comunicación en tiempo real, con diversos grados de anonimato. Los servicios de mensajería en línea consisten normalmente en comunicaciones bilaterales, mientras que las salas de charla ofrecen una comunicación abierta a un grupo de personas. La inscripción para usar los servicios de mensajería en línea generalmente se basa en información no verificada, proporcionada por el usuario; sin embargo, algunos

servicios de Internet también registran la dirección IP en uso en el momento de la inscripción, que puede ser solicitada por las autoridades encargadas de hacer cumplir la ley, sin perjuicio de las garantías jurídicas aplicables. Las comunicaciones se identifican generalmente por un nombre de usuario único, que puede ser asignado permanentemente al inscribirse el usuario o estar limitado a una sesión en línea en particular. El proveedor de servicios generalmente no guarda la información intercambiada durante una sesión de mensajería en línea y por tanto dicha información puede no estar disponible para la recuperación después de terminada la sesión en línea, aunque el análisis forense del disco duro de la computadora de uno de los interlocutores permitiría recuperarla.

189. Las salas de charla en línea protegidas por contraseña pueden ser usadas por las organizaciones terroristas y simpatizantes para promover un sentido de comunidad dentro de un entorno global. Los mensajes de las salas de charla pueden estar sujetos a una mayor monitorización —y ser guardados por el proveedor de servicios de mensajería— que los diálogos entre dos personas, lo cual aumenta las probabilidades de obtener pruebas documentales en una investigación¹¹⁴. En algunas jurisdicciones, el personal encargado de hacer cumplir la ley puede, con sujeción a ciertas condiciones, inscribirse secretamente, con un seudónimo, y participar en conversaciones de las salas de charla para los fines de la investigación.

190. Por ejemplo, en Francia, el artículo 706 del Código de Procedimiento Penal prevé que el fiscal o el juez de instrucción puede autorizar las operaciones de infiltración de este tipo en relación con delitos cometidos a través de comunicaciones electrónicas (véase la discusión del tema en la sección III. C. 3 a)). El objetivo de este tipo de operaciones puede ser, entre otras cosas, reunir inteligencia o, si se sospecha que existe una amenaza de un atentado terrorista, adoptar medidas proactivas para frustrarlo. Sin embargo, hay que tener sumo cuidado, al inicio de la operación, de asegurarse de que ninguna infiltración de sala de charla en línea o de otros foros de Internet se lleve a cabo de manera que permita a la defensa alegar que hubo inducción dolosa a la comisión de un delito, aduciendo que las autoridades indujeron al sospechoso a cometer un delito que no estaba predispuesto a cometer.

d) *Redes de intercambio de ficheros y tecnología informática en la nube*

191. Los sitios web de intercambio de ficheros, como Rapidshare, Dropbox o Fileshare, permiten a las partes cargar, compartir, localizar y acceder a ficheros multimedia por Internet con suma facilidad. Las técnicas de cifrado y de resguardo del anonimato empleadas en relación con otras formas de comunicación por Internet son igualmente aplicables a los ficheros compartidos a través de, entre otras cosas, la tecnología P2P y de protocolo de transferencia de ficheros (FTP). Por ejemplo, en la causa Hicheur (véase el párrafo 20 *supra*), se presentaron pruebas de que los ficheros digitales en apoyo de actividades terroristas habían sido compartidos mediante Rapidshare, después de ser cifrados y comprimidos para fines de seguridad. Algunas redes de intercambio

¹¹⁴Ibid., págs. 34 y ss.

de ficheros pueden mantener constancia de las transferencias o información sobre pagos, que pueden ser pertinentes en el contexto de una investigación.

192. La computación en nube es un servicio que proporciona a los usuarios acceso remoto a programas y datos almacenados o ejecutados en los servidores de datos de terceros. Al igual que con el intercambio de ficheros, la computación en nube proporciona un medio conveniente de almacenar, compartir y distribuir documentación en línea. El uso de la tecnología en la nube para acceder a información almacenada a distancia reduce la cantidad de datos almacenados localmente en los dispositivos individuales, junto con la capacidad correspondiente de recuperar posibles pruebas en las investigaciones del uso de Internet por terroristas.

193. Los servidores de datos utilizados para proporcionar estos servicios pueden estar ubicados físicamente en una jurisdicción diferente de la del usuario registrado, con niveles variables de capacidad de regulación y ejecución de la ley. Por consiguiente, en estos casos puede resultar necesaria una estrecha coordinación con las autoridades locales de aplicación de la ley para obtener pruebas clave para las actuaciones judiciales.

2. Técnicas de cifrado de datos y de resguardo del anonimato

194. El cifrado de datos se refiere a la protección de la información digital contra la divulgación mediante su conversión en texto cifrado, utilizando un algoritmo matemático y una clave de cifrado, de modo que sea inteligible solo para el destinatario legítimo. Los instrumentos de cifrado pueden consistir en equipo físico o en software, o en una combinación de ambos. Una vez cifrada la información, se necesita una contraseña, una frase de paso, una “clave de software” o un dispositivo físico de acceso, o una combinación de estos medios, para acceder a ella. El cifrado puede aplicarse tanto a los datos “en reposo”, contenidos en los dispositivos de almacenamiento, como los discos duros de las computadoras, las unidades de memoria y los teléfonos “inteligentes”, como a los datos “en tránsito”, transmitidos a través de Internet, por ejemplo por telefonía VoIP y correo electrónico. Algunos ejemplos comunes de herramientas de cifrado basadas en software son las integradas en los sistemas operativos o de aplicaciones de computadora, y programas informáticos independientes, como Pretty Good Privacy y WinZip¹¹⁵. En un caso del Brasil, se inició una investigación, sobre la base de la cooperación internacional y el intercambio de información, de una persona de quien se sospechaba que moderaba y controlaba las operaciones de un sitio web yihadista afiliado a reconocidas organizaciones terroristas, en particular Al-Qaida, en el que también participaba. Este sitio web hospedaba videos, documentos y mensajes de cabecillas extremistas, que habían sido traducidos al inglés para llegar a un público más amplio, y también se utilizaba para llevar a cabo actividades de recaudación de fondos y campañas de propaganda racista. La operación policial que llevó a la detención del sospechoso se concibió de modo que permitiera tomar al sospechoso por sorpresa, mientras

¹¹⁵Estados Unidos, Departamento de Justicia, Oficina de Programas Judiciales, Instituto Nacional de Justicia, *Investigative Uses of Technology: Devices, Tools and Techniques* (2007), pág. 50.

se encontraba conectado a Internet, participando activamente en las actividades del sitio web. Al aprehender al sospechoso mientras su computadora estaba encendida y abiertos los ficheros pertinentes, los investigadores pudieron sortear las claves criptográficas simétricas y otros obstáculos de cifrado y funciones de seguridad usados por el sospechoso y sus asociados. Los investigadores lograron, por tanto, acceder al contenido digital, que de otro modo podría haber sido inaccesible o más difícil de descifrar si la computadora hubiera estado apagada en el momento de la incautación.

195. Las actividades en Internet o la identidad de los usuarios asociados también pueden ocultarse mediante técnicas avanzadas, entre otras, la de encubrir la dirección IP de origen, usurpar la dirección IP de otro sistema o redirigir el tráfico de Internet a una dirección IP “oscurecida”¹¹⁶. Un servidor intermediario permite a los usuarios hacer conexiones de red indirectas con otros servicios de red. Algunos servidores intermediarios permiten que la configuración del navegador del usuario encamine de forma automática el tráfico del navegador a través de un servidor intermediario. Este solicita servicios de red en nombre del usuario y entonces encamina los resultados de nuevo a través de un servidor intermediario. El uso de servidores intermediarios permite alcanzar distintos niveles de anonimato. Un intermediario puede encubrir la identidad de un usuario formulando la solicitud de servicios de red sin revelar la dirección IP en que se origina la solicitud, o dando intencionalmente una dirección IP de origen incorrecta. Por ejemplo, pueden usarse aplicaciones como The Onion Router para proteger el anonimato de los usuarios reencaminando automáticamente la actividad en Internet a través de una red de servidores intermediarios con el fin de ocultar el punto de origen. El reencaminamiento del tráfico de red a través de varios servidores intermediarios, que pueden estar ubicados en jurisdicciones diferentes, aumenta el grado de dificultad de identificar con exactitud al autor de una transmisión.

196. Otro método consiste en infiltrarse en la dirección IP de una organización legítima y navegar por Internet usando la dirección pirateada. Todos los rastros de esa actividad quedarán vinculados a la dirección IP de la organización comprometida. Un sospechoso también puede acceder a un sitio web a través de una computadora comprometida o cargar un programa malicioso en un sitio web comprometido (usado, por ejemplo, para obtener información sobre tarjetas de crédito u otros datos financieros personales) en un intento de evitar ser identificado.

197. Hay una variedad de programas informáticos disponibles para encubrir o cifrar los datos transmitidos a través de Internet para fines ilícitos. Estos programas pueden incluir el uso de software como Camouflage para ocultar información mediante la esteganografía o el cifrado y la protección con contraseña de ficheros usando programas como WinZip. También se puede emplear el recurso de las capas múltiples de protección de datos. Por ejemplo, Camouflage permite ocultar ficheros mediante su aleatorización, tras lo cual se añaden al final de un fichero cualquiera de remisión. El fichero de remisión conserva sus propiedades originales, pero actúa como portador para almacenar o transmitir el archivo oculto. Este software se puede aplicar a una amplia gama de

¹¹⁶Instituto Nacional de Justicia, *Investigations Involving the Internet and Computer Networks*, pág. 9.

tipos de ficheros. Sin embargo, el fichero oculto puede ser detectado mediante un examen de los datos del fichero en bruto, lo que revelaría la existencia del archivo adjunto oculto¹¹⁷.

198. En el Reino Unido, la Ley de poderes de regulación de la investigación 2000 tipifica como delito el negarse a entregar una clave de cifrado cuando así lo exigen las autoridades. Se debe tener cuidado, con todo, de asegurarse de que los sospechosos no traten de eludir la disposición mediante la utilización de varias capas de cifrado y claves múltiples para proteger conjuntos de datos diferentes. Por ejemplo, un ajuste de TruCrypt, conocido instrumento gratuito de cifrado, permite a un sospechoso cifrar un disco duro y crear dos contraseñas: una para la unidad “limpia” y la otra para la que contiene el material incriminatorio. Esto se puede superar asegurándose de que en el examen forense de la unidad de disco duro se verifique si hay algún “volumen perdido” de datos. Además, las infracciones de esta naturaleza suelen ser faltas, que conllevan penas máximas de seis meses de prisión. En el Reino Unido, empero, cuando la falta está relacionada con cuestiones de seguridad nacional, la pena máxima aumenta a dos años de prisión.

3. Tecnología inalámbrica

199. La tecnología de redes inalámbricas permite a las computadoras y otros dispositivos acceder a Internet mediante una señal de radio en lugar de una conexión por cable. Para acceder a una red inalámbrica (Wi-Fi), debe mantenerse cierta proximidad física a los recursos de la red, lo que depende de la intensidad de la señal inalámbrica. Las redes inalámbricas pueden configurarse para permitir el acceso abierto a Internet, sin necesidad de inscribirse, o se puede restringir el acceso mediante el uso de una contraseña o niveles de cifrado variables. En general, se puede acceder a las redes inalámbricas, registradas a nombre de particulares, empresas o entidades públicas, desde lugares públicos. El acceso anónimo a redes inalámbricas abiertas o protegidas puede permitir a un infractor ocultar los vínculos entre su actividad en Internet y los datos que lo identifican.

200. Además, en los últimos años han surgido proveedores de servicios tales como Fon, que permiten a los usuarios registrados compartir parte de su ancho de banda de la red inalámbrica residencial con otros abonados, a cambio del acceso recíproco a redes inalámbricas de abonados en todo el mundo. Las actividades realizadas en una red inalámbrica compartida complica considerablemente el proceso de atribución de un hecho a un autor único, identificable, en el curso de una investigación¹¹⁸.

201. Una nueva técnica se basa en la utilización de receptores de radio de alta frecuencia de alto rendimiento, definidos por software, en que los mensajes son encaminados por una computadora. De esta manera, no se intercambian datos a través de un servidor ni se crean registros. Es más difícil para la policía y los servicios de inteligencia

¹¹⁷Comunicación escrita del experto del Raggruppamento Operativo Speciale de los Carabinieri de Italia.

¹¹⁸Ibid.

interceptar las comunicaciones establecidas por este método, tanto en relación con la localización de los transmisores como con respecto a la predicción en tiempo real de la frecuencia en que se envían los mensajes.

B. Investigaciones de casos de terrorismo en que se usó Internet

I. Enfoque sistemático de las investigaciones del uso de Internet

202. Existe una extensa gama de datos y servicios disponibles en Internet que se pueden emplear en una investigación para contrarrestar el uso de Internet por terroristas. Un enfoque proactivo de las estrategias de investigación y herramientas de apoyo especializadas permite aprovechar los recursos de Internet en evolución a fin de determinar de manera eficiente qué datos y qué servicios son los que pueden producir el máximo beneficio para la investigación. En reconocimiento de la necesidad de un enfoque sistemático de la utilización de los avances tecnológicos relacionados con Internet para los fines de la investigación, el Raggruppamento Operativo Speciale de los Carabinieri de Italia formuló las siguientes directrices, que se han difundido a través de la Universidad de Dublín, con su programa de maestría en informática forense y ciberdelincuencia (véase la sección IV.G *infra*) y han sido llevadas a la práctica por las autoridades policiales nacionales de muchos Estados miembros de la Organización Internacional de Policía Criminal (INTERPOL) y la Oficina Europea de Policía (Europol):

Protocolo de un enfoque sistemático

- *Reunión de datos*: Esta fase consiste en la reunión de datos por los métodos tradicionales de investigación, como la obtención de información sobre el sospechoso de cualquier cohabitante, los compañeros de trabajo pertinentes y otros asociados, y la información obtenida mediante las actividades convencionales de monitorización de canales de comunicación, en particular las líneas telefónicas fijas y móviles.
- *Búsqueda de la información adicional disponible en servicios basados en Internet*: Esta fase incluye solicitudes para obtener la información recogida y almacenada en las bases de datos de los servicios de comercio electrónico, de comunicaciones y de red basados en la web, tales como eBay, PayPal, Google y Facebook, así como el uso de buscadores especializados como www.123people.com. Los datos recogidos por estos servicios mediante los conocidos "cookies" de Internet también proporcionan información clave sobre los múltiples usuarios de una misma computadora o dispositivo móvil.
- Las actividades de las fases a) y b) anteriores proporcionan datos que pueden combinarse y ser sometidos a una referencia cruzada para trazar un perfil de la persona o grupo de personas investigadas y ponerlo a disposición de los investigadores para el análisis en las últimas etapas de la investigación.
- *Solicitudes al proveedor de servicios VoIP*: En esta fase, las autoridades policiales solicitan información a los proveedores de servicios VoIP sobre las personas objeto de la investigación y cualquier otro asociado o usuario conocido de los mismos dispositivos de red. La información recogida en esta fase también puede ser utilizada como una forma de "filtro inteligente" a los efectos de verificar la información obtenida en las dos fases anteriores.

- *Análisis*: El gran volumen de datos obtenidos de los servidores VoIP y los proveedores de diversos servicios de Internet se analiza a continuación para determinar qué datos y tendencias son más útiles para la investigación. Este análisis puede ser facilitado por programas informáticos, que pueden filtrar información o proporcionar representaciones gráficas de los datos digitales obtenidos para destacar, entre otras cosas, las tendencias, la cronología, la existencia de un grupo organizado o jerarquía, la ubicación geográfica de los miembros del grupo, o los factores comunes a varios usuarios, por ejemplo: una fuente común de financiación.
- *Identificación de personas de interés*: En esta fase, tras el análisis selectivo de los datos, es común identificar a las personas de interés basándose, por ejemplo, en la información sobre los abonados relacionada con una cuenta financiera, de VoIP o de correo electrónico.
- *Actividad de interceptación*: En esta fase, las autoridades policiales emplean tácticas de interceptación similares a las utilizadas para los canales de comunicación tradicionales, pero trasladándolas a una plataforma diferente: los canales digitales de comunicación. La actividad de interceptación puede llevarse a cabo en relación con los servicios de telecomunicaciones, como las comunicaciones de banda ancha fija, banda ancha móvil e inalámbricas, así como con respecto a los servicios prestados por proveedores de servicios de Internet tales como los servicios de comunicación de correo electrónico, de charlas y foros. En particular, en los últimos años, la experiencia ha puesto de manifiesto ciertas vulnerabilidades en las nuevas tecnologías de la comunicación que pueden ser explotadas con fines de investigación o reunión de inteligencia. Debe procederse con el debido cuidado en cuanto a garantizar la integridad forense de los datos recogidos y a corroborar, en la medida de lo posible, la inteligencia reunida con identificadores objetivos como las coordenadas del sistema mundial de determinación de posición (GPS), sellos de fecha y hora o videos de vigilancia.

Cuando lo permita el derecho interno, algunas autoridades policiales también podrán emplear técnicas digitales de monitorización facilitadas por la instalación de dispositivos físicos o de aplicaciones informáticas como un virus, un "caballo de Troya" o un capturador de teclado en la computadora de la persona investigada. Esto se puede lograr mediante el acceso directo o remoto a la computadora pertinente, teniendo en cuenta el perfil técnico del hardware que ha de infiltrarse (tales como la presencia de protecciones antivirus o cortafuegos) y el perfil personal de todos los usuarios del dispositivo, dirigiendo el ataque contra el perfil de usuario menos avanzado.

203. La Policía Nacional de Corea ha respondido a la necesidad de uniformar las prácticas nacionales de la policía relativas al análisis forense digital mediante el desarrollo y la difusión de dos manuales: *Directrices uniformes para el tratamiento de pruebas digitales* y el *Manual técnico de análisis forense digital*. Las *Directrices uniformes* detallan siete pasos en el tratamiento adecuado de las pruebas digitales: preparación; reunión; examen; solicitud, recepción y transporte de las pruebas; análisis; presentación de informes, y conservación y gestión de las pruebas. El *Manual técnico de análisis forense digital* describe los procedimientos necesarios y el enfoque más indicado para la reunión de pruebas digitales, incluso en relación con el establecimiento del entorno, las herramientas forenses y el equipo apropiados; medidas preparatorias, tales como la configuración del hardware y software, conexiones de red y cronología exacta; medidas

para asegurar la máxima cantidad de pruebas digitales; el análisis independiente de los datos incautados, y la preparación del informe final¹¹⁹.

2. Rastreo de una dirección IP

204. La dirección IP asociada a una comunicación de Internet es un identificador importante, y clave, por tanto, en las investigaciones del uso de Internet por terroristas. La dirección IP identifica la red y el dispositivo específicos usados para acceder a Internet. Las direcciones IP pueden ser dinámicas, asignadas temporalmente por la duración de una sesión en línea y tomadas de un grupo de direcciones disponibles para un proveedor de servicios de Internet o estáticas (asignadas sobre una base fija, como en el caso de las direcciones de los sitios web). Las direcciones IP dinámicas se suelen asignar al proveedor de servicios de Internet en bloques basados en regiones geográficas. Por consiguiente, si no se han usado técnicas de resguardo del anonimato o de otro tipo, una dirección IP dinámica a menudo puede usarse para identificar la región o el Estado desde donde una computadora se conecta a Internet.

205. Además, en respuesta a una solicitud debidamente formulada, un proveedor de servicios de Internet a menudo puede determinar cuál de las cuentas de sus abonados estaba asociada con una dirección IP en un momento dado. Pueden usarse entonces los métodos de investigación tradicionales para identificar a la persona con el control físico de la cuenta de abonado en ese momento. En el caso *Hicheur* (véase el párrafo 20 *supra*), el acusado fue identificado mediante el rastreo de una dirección IP estática usada para acceder a una cuenta de correo electrónico bajo vigilancia. Una solicitud dirigida al proveedor de servicios de Internet pertinente permitió a las autoridades vincular la dirección IP a una cuenta de abonado usada por múltiples ocupantes de una casa, incluido el acusado. Interceptando los datos de tráfico de esta cuenta de abonado, los investigadores también lograron establecer vínculos entre la dirección IP y la actividad de un sitio web yihadista que distribuía, entre otras cosas, materiales para adiestrar a combatientes extremistas física y psicológicamente. En particular, los investigadores lograron correlacionar las horas en que se establecían múltiples conexiones con el foro de discusión del sitio web con un aumento concomitante del volumen de datos en Internet relacionados con la cuenta de correo electrónico personal del acusado¹²⁰.

206. Dada la importancia del factor tiempo en las investigaciones relacionadas con Internet y el riesgo de alteración o supresión de los datos digitales debido, entre otras cosas, a las posibles limitaciones de la capacidad del servidor del proveedor de servicios de Internet pertinente o las normas aplicables de protección de datos, debe tenerse muy en cuenta la conveniencia de solicitar al proveedor de servicios de Internet que conserve los datos pertinentes para la investigación penal, mientras se satisfacen los requisitos necesarios para obtener los datos con fines probatorios.

¹¹⁹Comunicación escrita del experto de la República de Corea.

¹²⁰Sentencia de 4 de mayo de 2012, Causa núm. 0926639036 del Tribunal de Grande Instance de París (14a Sala/2), pág. 7 y ss.

207. En el caso de una investigación relacionada con un sitio web, debe determinarse primero qué dirección IP corresponde al nombre de dominio en cuestión. A fin de identificar la dirección IP asociada, que a su vez se ha registrado en la Corporación de Internet para la Asignación de Nombres y Números (ICANN), puede recurrirse a varias aplicaciones especiales de búsqueda. Las aplicaciones más conocidas disponibles en Internet incluyen “whois” y “nslookup”¹²¹. Por ejemplo, una consulta whois relacionada con el nombre de dominio de la Oficina de las Naciones Unidas contra la Droga y el Delito (www.unodc.org) produce el siguiente resultado:

Identidad del dominio: D91116542-LROR
Nombre del dominio: UNODC.ORG
Creado en: 11-oct-2002 09:23:23 Hora universal coordinada (HUC)
Actualizado por última vez: 19-oct-2004 00:49:30 HUC
Fecha de vencimiento: 11-oct-2012 09:23:23 HUC
Registro patrocinador: Network Solutions LLC (R63-LROR)
Estado: PROHIBIDA LA TRANSFERENCIA A OTRO CLIENTE
Identidad del titular registrado: 15108436-NSI
Nombre del titular registrado: Wiessner Alexander
Organización registrada: United Nations Vienna
Calle1 del titular registrado: Vienna International Centre, P.O. Box 500
Ciudad del titular registrado: A-1400 Wien Vienna AT 1400
Código postal del titular registrado: 99999
País del titular registrado: AT
Teléfono del titular registrado: +43.1260604409
FAX del titular registrado: +43.1213464409
Correo electrónico del titular registrado: noc@unvienna.org

Sin embargo, esta información es proporcionada por el titular registrado. Por consiguiente, puede resultar necesario tomar medidas adicionales para verificar independientemente la exactitud de los datos del titular registrado. Además, los dominios se pueden arrendar o estar bajo el control de una parte que no sea el titular registrado.

208. Los investigadores del uso de Internet con fines terroristas también deben ser conscientes de que su propia actividad en línea relacionada con una investigación puede ser monitorizada, registrada y rastreada por terceros. Por consiguiente, es preciso tener especial cuidado de evitar hacer indagaciones en línea desde equipo que pueda rastrearse a la organización investigadora¹²².

¹²¹ Instituto Nacional de Justicia, *Investigations Involving the Internet and Computer Networks*, pág. 10.

¹²² *Ibid.*

3. Aplicaciones y hardware especializados para la investigación

209. Los investigadores con una adecuada formación técnica tienen a su disposición una amplia gama de aplicaciones de búsqueda y de hardware especializados. Algunos, tales como “Ping” y “Traceroute”, pueden estar integrados en el sistema operativo de un dispositivo investigado. Ping, por ejemplo, puede usarse para enviar una señal a una computadora conectada a Internet para determinar si está conectada en un momento dado, protegida por cortafuegos u otras configuraciones de la red. Del mismo modo, Traceroute puede indicar la ruta entre dos computadoras conectadas en una red, lo que puede ayudar a determinar la ubicación física.

210. Otros programas que pueden usarse, dentro de los límites fijados por las leyes y los reglamentos internos relativos, entre otras cosas, al acceso a dispositivos y la interceptación de las comunicaciones, son los “caballos de Troya” o Troyanos de Administración Remota (RAT o “ratas”), que pueden ser introducidos clandestinamente en un sistema informático para reunir información o para permitir el control remoto de la computadora afectada. También pueden instalarse en un dispositivo detectores de teclado para monitorizar y registrar la actividad del teclado. Los capturadores de teclado, en forma de hardware o software, ayudan a obtener información, entre otras cosas, sobre contraseñas, comunicaciones y la actividad en sitios web o localizada gracias al dispositivo monitorizado. Además, pueden usarse rastreadores de paquetes de datos (“sniffers”) para reunir información en una investigación. Estos rastreadores, que pueden ser dispositivos físicos o software, obtienen la información directamente desde una red y pueden proporcionar información sobre la fuente y el contenido de las comunicaciones.

C. Técnicas forenses de preservación y recuperación de datos

211. Una parte importante de la obtención de pruebas en relación con los casos de uso de Internet con fines terroristas se refiere a la recuperación de los datos digitales almacenados. Los dos objetivos principales de esta operación de recuperación de datos son la recuperación de los elementos de prueba pertinentes para los fines de la investigación y el enjuiciamiento eficaces y la preservación de la integridad de la fuente de datos y la cadena de custodia para garantizar su admisibilidad en juicio. Si se quiere determinar cuál es el mejor método de preservación de las pruebas, es importante distinguir entre los datos volátiles, que están almacenados en dispositivos, tales como la memoria de acceso aleatorio (RAM) de una computadora, que pueden perderse irremisiblemente si hay una interrupción en el suministro de electricidad, y los datos no volátiles, que se mantienen independientemente de la fuente eléctrica del dispositivo. Por ejemplo, el acto de apagar una computadora puede alterar los datos contenidos en los discos de almacenamiento y la memoria RAM, que pueden contener pruebas importantes de los programas informáticos usados por el sospechoso o los sitios web visitados. Los datos volátiles pueden proporcionar información sobre los procesos en curso en una computadora activa, lo cual puede ser útil en una investigación, tales como información sobre los usuarios, contraseñas, datos no cifrados o mensajes instantáneos. Ejemplos de dispositivos de almacenamiento de datos no volátiles son, entre otros, los discos duros internos y externos, las unidades de memoria portátiles, los dispositivos de almacenamiento flash y los discos de compresión (discos Zip).

212. El Departamento de Seguridad Nacional de los Estados Unidos ha preparado una valiosa sinopsis de este proceso en una guía titulada “Best practices for seizing electronic evidence: a pocket guide for first responders”¹²³ (Las mejores prácticas para incautarse de pruebas electrónicas: guía de bolsillo para socorristas). Esta guía describe los siguientes pasos para preservar las pruebas en las investigaciones penales relacionadas con los dispositivos de computación:

Las mejores prácticas de preservación de los datos

- No use la computadora ni trate de buscar elementos de prueba
- Si el equipo está conectado a una red, desconecte la fuente eléctrica del encaminador (router) o módem
- Antes de mover cualquier elemento de prueba, fotografíe la computadora como se encuentra, incluidas la parte de adelante y la de atrás, así como todos los cables o dispositivos conectados y el área circundante
- Si la computadora está apagada, no la encienda
- Si la computadora está encendida y se ve algo en el monitor, fotografíe la pantalla
- Si el equipo está encendido y la pantalla está en blanco, mueva el ratón o pulse la barra de espacio (esto traerá la imagen activa a la pantalla); una vez aparezca la imagen, fotografíe la pantalla
- En el caso de computadoras de escritorio, desenchufe el cable de alimentación de la parte de atrás de la torre de la computadora
- Si se trata de computadoras portátiles, desenchufe el cable de alimentación; si la computadora portátil no se apaga, localice y retire la batería (la batería está situada normalmente en la parte inferior y, por lo general, hay un botón o mecanismo de apertura que permite retirarla); una vez retirada la batería, no vuelva a colocarla en la computadora portátil (esto evitará que arranque por accidente)
- Diagrame y rotule los cables para poder identificar después los dispositivos conectados
- Desconecte todos los cables y dispositivos de la torre o computadora portátil
- Empaquete y transporte los componentes (incluidos el encaminador (router) y el módem, si está presente) como carga frágil
- Cuando esté permitido de conformidad con las condiciones de cualquier orden de registro aplicable, incáutese de cualquier otro medio de almacenamiento
- Mantenga todos los dispositivos, incluida la torre, lejos de imanes, radiotransmisores y otros elementos potencialmente dañinos
- Recoja los manuales de instrucciones, documentación y notas, prestando especial atención a todos los elementos que puedan revelar contraseñas o frases de paso usadas en computadoras
- Documente todos los pasos de la operación de incautarse de una computadora y sus componentes.

¹²³Estados Unidos, Departamento de Seguridad Nacional, “Best practices for seizing electronic evidence: a pocket guide for first responders”, 3a ed. (2007). Puede consultarse en www.forwardedge2.com/pdf/bestPractices.pdf.

213. Con respecto a los dispositivos móviles, tales como teléfonos “inteligentes” y asistentes digitales personales, se aplican principios similares, salvo que no se recomienda apagar el dispositivo, ya que esto puede habilitar la protección mediante contraseña, impidiendo el acceso a las pruebas. El dispositivo, por tanto, debe mantenerse cargado, en la medida de lo posible, o someterlo al análisis por un especialista tan pronto como sea posible, antes de que la pila se descargue, para evitar la pérdida de datos.

214. El siguiente caso de la India ilustra la importancia del análisis forense en la identificación y recuperación de pruebas digitales y de otro tipo en las investigaciones del uso de Internet por terroristas.

La causa Zia Ul Haq

El acusado, Zia Ul Haq, detenido el 3 de mayo de 2010 y actualmente en espera de juicio, es presuntamente miembro de Lashker e Taiba, grupo armado con base en el Pakistán que lucha contra el control indio de Cachemira. La acusación contra Zia Ul Haq alega, entre otras cosas, que fue atraído a la yihad mientras trabajaba en la Arabia Saudita entre 1999 y 2001; recibió adiestramiento, fuera de la India, en el uso de armas, municiones y explosivos y mantuvo sus contactos por correo electrónico; recibió un envío de armas, municiones y explosivos en Delhi en 2005, después de que se le pidiera por correo electrónico que lo recibiera, y posteriormente usó Internet para coordinar con otros miembros de Lashker e Taiba y se confabuló para cometer actos terroristas con armas, municiones y explosivos.

La fiscalía alega que el 7 de mayo de 2006, Zia Ul Haq utilizó granadas de mano suministradas como parte del envío de armas de Lashker e Taiba en un atentado contra el cine Odeón, en Hyderabad.

Se obtuvieron de los proveedores de servicios de Internet comunicaciones por correo electrónico entre el acusado y su entrenador y se examinó su contenido. Las computadoras de los cibercafés usadas por el delincuente se sometieron a un análisis forense; se localizó el hotel donde se había alojado durante su estancia en Delhi para recoger las granadas y se determinó por métodos forenses que la firma que aparecía en el registro de huéspedes era la suya. Mientras el acusado estaba preso en espera de juicio, se envió una carta rogatoria desde la India a la autoridad central de otro país para iniciar una acción contra el presunto entrenador.

Zia Ul Haq fue acusado en la India de diversos delitos, incluidos los reprimidos en los artículos 15, 16, 17 y 18 de la Ley sobre (prevención de) actividades ilícitas de 1967, modificada en 2004 y 2008, que prevé el castigo de actividades terroristas, el adiestramiento y el reclutamiento con fines terroristas, la recaudación de fondos para actividades terroristas y la confabulación para cometer actos terroristas.

215. Debido a la fragilidad de las pruebas digitales, lo mejor es dejar su evaluación, obtención y análisis al cuidado de expertos forenses con formación especial. En Israel, la legislación nacional reconoce la importancia de la formación especializada y dispone que las pruebas digitales sean obtenidas por investigadores capacitados en informática, que hacen un curso básico profesional y reciben formación profesional avanzada en el servicio para familiarizarse con los sistemas informáticos, los diversos programas informáticos forenses y la forma óptima de usarlos. Cuando surge la necesidad de una investigación especialmente compleja, como la recuperación de ficheros borrados,

defectuosos o encubiertos o cifrados con claves complejas, puede contratarse a un experto externo, que más tarde puede ser llamado a declarar como testigo pericial de cargo¹²⁴.

216. Es aconsejable llevar a cabo todos los exámenes en copias de los elementos de prueba originales, con el fin de preservar la integridad de los datos originales¹²⁵. Puede crearse un duplicado de los datos digitales usando determinadas herramientas forenses, tales como EnCase, de Guidance Software, o Forensic Tool Kit, u otros programas gratuitos (freeware). En la medida de lo posible, deberían usarse al menos dos instrumentos forenses diferentes para crear duplicados, en caso de que uno de ellos no recoja adecuadamente todos los datos¹²⁶.

217. EnCase proporciona una imagen duplicada de los datos del dispositivo en estudio, analiza todos los sectores del disco duro, incluidos los sectores no asignados, para asegurar la captura de ficheros ocultos o borrados. El software también puede ser utilizado, entre otras cosas, para analizar la estructura del sistema de ficheros de los medios digitales, organizar los ficheros analizados y generar una representación gráfica u otro informe sobre ciertas características de los ficheros. EnCase también genera y asigna un identificador único, el llamado “valor hash”, a las pruebas digitales¹²⁷.

218. Con el fin de validar la autenticidad de las pruebas digitales en el marco de actuaciones judiciales (véase la sección IV.D *infra*), se asigna un valor hash a los archivos digitales, o a partes de estos, basado en un algoritmo matemático aplicado a las características del conjunto de datos. Cualquier alteración del conjunto de datos daría lugar a la generación de un valor hash diferente. Se generan valores hash con respecto a *a)* el disco duro original antes de la creación de una imagen duplicada, *b)* el duplicado o los duplicados antes del examen forense y *c)* el duplicado o los duplicados después de su examen. La coincidencia de los valores hash corrobora la conclusión de que no se han manipulado las pruebas digitales y la copia objeto de examen forense puede ser tratada como los datos originales a efectos de las actuaciones judiciales. Los algoritmos comúnmente utilizados son MD5 y SHA¹²⁸.

D. Validación de la autenticidad de las pruebas digitales

219. La persecución eficaz de un presunto caso de uso de Internet para fines terroristas debe descansar en elementos de prueba recogidos correctamente y bien documentados

¹²⁴Comunicación escrita del experto de Israel.

¹²⁵Estados Unidos, Departamento de Justicia, Oficina de Programas Judiciales, Instituto Nacional de Justicia, *Forensic Examination of Digital Evidence: A Guide for Law Enforcement* (2004), pág. 1. Puede consultarse en www.ncjrs.gov/pdffiles1/nij/199408.pdf.

¹²⁶EC-Council Press, *Computer Forensics: Investigating Data and Image Files* (Clifton Park, Nueva York, Course Technology Cengage Learning, 2010), págs. 2 a 4.

¹²⁷Comunicación escrita del experto del Raggruppamento Operativo Speciale de los Carabinieri de Italia.

¹²⁸Barbara J. Rothstein, Ronald J. Hedges y Elizabeth C. Wiggins, “Managing discovery of electronic information: a pocket guide for judges” (Federal Judicial Center, 2007). Puede consultarse en [www.fjc.gov/public/pdf.nsf/lookup/eldscpkt.pdf/\\$file/eldscpkt.pdf](http://www.fjc.gov/public/pdf.nsf/lookup/eldscpkt.pdf/$file/eldscpkt.pdf).

(véase la sección VI.G.2 *infra*). Esto es necesario para establecer la integridad de las pruebas digitales, para los fines tanto de su admisibilidad en juicio como por su valor persuasivo. La integridad de las pruebas digitales puede establecerse mediante una combinación de técnicas de investigación tradicionales y especializadas. Los aspectos clave incluyen la cadena de custodia, tanto del dispositivo físico utilizado para almacenar o transmitir datos electrónicos como de los datos mismos, así como los procedimientos seguidos para obtener dichos datos y cualquier desviación de los procedimientos establecidos. Con respecto a los métodos de investigación tradicionales, los agentes de policía pueden hacer indagaciones para establecer, en la medida de lo posible, quién pudo haber manejado o tenido acceso a las pruebas antes de ser detenido y cuándo, cómo y dónde se recogieron las pruebas.

220. El fiscal también puede verse en la necesidad de demostrar, entre otras cosas, que la información obtenida es una representación verdadera y exacta de los datos originalmente contenidos en los medios de comunicación y que pueden atribuirse a los acusados. Los valores hash generados con respecto a las pruebas digitales proporcionan una sólida corroboración de que las pruebas se mantienen intactas. También se pueden presentar pruebas y testimonios adicionales que corroboren y establezcan la autenticidad. Un ejemplo de esta práctica se puede encontrar en el caso de Adam Busby, condenado en Irlanda en 2010 por enviar una amenaza de atentado con bomba por correo electrónico al aeropuerto de Heathrow en Londres. Durante el juicio de Busby, además de presentar pruebas de que el mensaje electrónico había sido enviado desde una computadora concreta a la que el acusado tenía acceso, también se presentaron registros informáticos impresos e imágenes de televisión de circuito cerrado con subtítulos para determinar el momento en que había sido transmitido el mensaje y el hecho de que el acusado era la persona con control de la computadora en ese momento.

E. Dependencias operacionales de lucha contra la ciberdelincuencia

1. Dependencias nacionales o regionales de lucha contra la ciberdelincuencia

221. El uso cada vez mayor de la tecnología informática ha dado lugar a un aumento espectacular de la demanda de dependencias especializadas en delitos informáticos para responder a las solicitudes de recuperación forense de pruebas informáticas, y no solo en casos de terrorismo con uso de Internet. La delincuencia organizada como el narcotráfico, la trata de personas y los grupos internacionales de pedófilos ofrece ejemplos de casos en que el uso delictivo de Internet ha sido muy frecuente, pero en años recientes ha habido un aumento en el grado en que los casos entrañan algún tipo de pruebas relacionadas con computadoras o pruebas electrónicas. El establecimiento de dependencias nacionales de lucha contra la ciberdelincuencia con conocimientos especializados en la investigación de los delitos cibernéticos podría aumentar considerablemente la capacidad operacional del Estado para satisfacer la demanda. Según los factores geográficos y las necesidades de recursos, esas dependencias nacionales también podrían recibir apoyo de dependencias regionales más pequeñas para responder a las necesidades locales. Además, es posible que resulte más eficiente y rentable tener dependencias regionales a cargo de administraciones regionales locales.

222. Las funciones de las dependencias nacionales o regionales de lucha contra la ciberdelincuencia podrían ser, entre otras, las siguientes:

- a) Reunión de inteligencia de fuentes abiertas mediante el uso de técnicas especiales de vigilancia en línea de los sitios de redes sociales, salas de charla, sitios web y tableros de anuncios de Internet que revelan las actividades de grupos terroristas (entre muchos otros elementos delictivos). Por lo que a los grupos terroristas se refiere, esta función podría ser una de las atribuciones de las dependencias de lucha contra el terrorismo que tengan personal con formación y experiencia suficientes para llevar a cabo esta tarea, pero la formación especializada en un entorno de ciberdelincuencia se considera esencial para desempeñar este papel. La función de reunión de inteligencia también exige evaluación y análisis para contribuir a la formulación de la estrategia de lucha contra la amenaza que plantea el uso de Internet por terroristas. El conflicto de responsabilidades u objetivos entre los organismos nacionales de inteligencia puede, no obstante, dificultar la armonización y el paso de las pistas de inteligencia a planes operacionales eficaces;
- b) Realización de investigaciones especializadas en ciberdelincuencia de casos nacionales e internacionales de comisión de delitos con uso de tecnologías avanzadas, como los delitos relacionados con el fraude en Internet o el robo de datos y otros casos en que se plantean complejos problemas de tecnología, derecho y procedimiento, y la administración de la dependencia de ciberdelincuencia determina que son necesarios los recursos de investigación especializada de dicha dependencia;
- c) Función de enlace internacional y con distintos sectores de la economía para el establecimiento de alianzas con los principales interesados en la lucha contra la ciberdelincuencia, como el sector de los servicios financieros, el sector de los servicios de telecomunicaciones, el sector de la computación, los departamentos pertinentes del gobierno, las instituciones académicas y las organizaciones intergubernamentales o regionales;
- d) Mantenimiento de una dependencia de evaluación para evaluar los casos de ciberdelincuencia a nivel nacional e internacional a fin de priorizar las investigaciones de las dependencias de ciberdelincuencia nacionales o regionales. Dicha dependencia también podría encargarse de llevar estadísticas sobre la incidencia de los casos de ciberdelincuencia;
- e) Actividades de formación, investigación y desarrollo, ya que la compleja y cambiante naturaleza de la ciberdelincuencia requiere el apoyo científico de las instituciones académicas especializadas para garantizar que las dependencias nacionales y regionales estén debidamente calificadas y dotadas de todas las herramientas tecnológicas, de formación y de educación necesarias para hacer análisis forenses de dispositivos informáticos e investigar la ciberdelincuencia.

2. Dependencias de triaje forense informático

223. Pueden establecerse dependencias de triaje forense informático para apoyar a las dependencias de ciberdelincuencia nacionales y regionales. El personal de estas dependencias estaría capacitado para hacer exámenes forenses de dispositivos informáticos, en el lugar donde se efectúa el registro, usando instrumentos de software especialmente diseñados. Un miembro del equipo de triaje puede llevar a cabo un primer examen sobre el terreno para eliminar cualquier computadora u otro equipo periférico de la investigación que no tenga valor probatorio o bien puede incautarse de las pruebas informáticas, de conformidad con las técnicas forenses correctas, y ayudar a los equipos locales de investigación en el interrogatorio de sospechosos en cuanto a las pruebas informáticas descubiertas. Cuando sea necesario, los elementos de los medios informáticos incautados por las dependencias de triaje también podrán derivarse a la dependencia regional o nacional de ciberdelincuencia competente para un examen forense completo, según proceda.

224. Los investigadores de la Universidad de Dublín están trabajando actualmente en el desarrollo de una serie de instrumentos de software forense para facilitar los análisis preliminares, instrumentos que estarán a disposición de los funcionarios encargados de hacer cumplir la ley sin ningún costo. El desarrollo de estos instrumentos es parte de una solución estratégica más amplia que exploran actualmente el Centro de Investigaciones sobre la Seguridad y la Delincuencia Cibernéticas de la Universidad de Dublín y la Dependencia de Investigación de Delitos Informáticos de An Garda Síochána (el Servicio Nacional de Policía de Irlanda), con objeto de ayudar a las dependencias de ciberdelincuencia con presupuestos limitados y que carecen de suficientes recursos y personal, en la gestión del volumen de trabajo. El objetivo de esta iniciativa será la creación de un laboratorio forense íntegramente de “código abierto”. Los investigadores participantes recibirán instrucción en la construcción de equipo de almacenamiento y de procesamiento de elementos de prueba informáticos, y serán capacitados en el uso de instrumentos forenses gratuitos.

F. Reunión de inteligencia

225. La reunión de inteligencia es un componente clave de las actividades de lucha contra el terrorismo, pues la información obtenida de este modo muchas veces pone en marcha investigaciones que llevan al enjuiciamiento de los sospechosos, o se utiliza como prueba en el juicio, en la medida permitida por la legislación y las normas de procedimiento nacionales. Sin embargo, las distintas finalidades para las que se reúne la inteligencia, y los diferentes organismos que pueden obtener o utilizar esta información, pueden obligar a buscar el justo equilibrio entre intereses en conflicto. Por ejemplo, los servicios de policía o de inteligencia dedicados a la obtención de inteligencia pueden hacer especial hincapié en la protección de la confidencialidad de la fuente de la información, mientras que los funcionarios judiciales tendrán que considerar, entre otras cosas, el derecho del acusado a un juicio imparcial y a un acceso igual a las pruebas presentadas en su contra. Se debe poner el debido cuidado en asegurarse de

que haya un sistema de control adecuado para proteger los derechos humanos fundamentales consagrados en las convenciones internacionales aplicables¹²⁹.

226. En algunos Estados Miembros, la inteligencia procedente de fuentes anónimas no es admisible como prueba en los tribunales; sin embargo, los datos de inteligencia corroborados por fuentes autorizadas o por otras pruebas pueden admitirse. Por ejemplo, en Irlanda, los datos de inteligencia reunidos sobre terroristas pueden constituir indicios racionales de que una determinada persona es miembro de una organización ilegal cuando esos indicios son presentados bajo juramento por un funcionario policial con un rango de al menos comisario principal. El Tribunal Supremo irlandés confirmó la admisibilidad de datos de inteligencia como prueba, en presencia de otras pruebas que los corroboren, cuando el temor a las represalias hace imposible el testimonio directo y el testigo que presta declaración es un funcionario de alto rango¹³⁰.

227. Varios expertos han puesto de relieve el conflicto existente entre la necesidad de fomentar la disponibilidad de información sobre posibles actividades terroristas realizadas a través de Internet y la necesidad de detener y procesar a los responsables de dicha actividad. Por ejemplo, una vez que se descubre una actividad de un sitio web potencialmente relacionada con el terrorismo, los organismos nacionales de seguridad pueden considerar las consecuencias a largo plazo y a corto plazo de la respuesta operacional. Esta respuesta puede consistir en la simple monitorización pasiva de la actividad del sitio web para fines de inteligencia, o la asignación de un agente encubierto para que interactúe con otros usuarios a fin de obtener más información con fines antiterroristas o el cierre del sitio web. Los distintos objetivos y estrategias de los diferentes organismos nacionales y extranjeros pueden orientar los métodos preferidos de lucha contra el terrorismo¹³¹.

228. En un reciente informe del Servicio de Investigación del Congreso de los Estados Unidos se pusieron de relieve las consideraciones prácticas de contraponer, por un lado, el valor de la inteligencia reunida y, por el otro, el peligro de la amenaza creada por un recurso en línea:

Según se informa, la [Agencia Central de Inteligencia] y el Gobierno de la Arabia Saudita diseñaron un sitio web yihadista, a manera de señuelo, para atraer a terroristas al sitio y monitorizar sus actividades. La información reunida en el sitio web fue usada por los analistas de inteligencia para seguir los planes operacionales de los yihadistas y detenerlos antes de que pudieran ejecutar los ataques planeados. Sin embargo, el sitio web también se usaba, según se informa, para transmitir los planes operacionales para los yihadistas que entraban en el Iraq para llevar a cabo ataques contra las tropas estadounidenses. Tras una serie de debates [entre los

¹²⁹Véanse, por ejemplo, la Declaración Universal de Derechos Humanos, art. 10; el Pacto Internacional de Derechos Civiles y Políticos, art. 14; y el Convenio para la Protección de los Derechos Humanos y las Libertades Fundamentales, art. 6.

¹³⁰*People (DPP) c. Kelly*, [2006] 3 I. R. 115.

¹³¹Catherine Theohary y John Rollins, Congressional Research Service (Estados Unidos), "Terrorist use of the Internet: information operations in cyberspace" (8 de marzo de 2011), pág. 8.

representantes de la Agencia de Seguridad Nacional, la Agencia Central de Inteligencia, el Departamento de Defensa, la Oficina del Director de Inteligencia Nacional y el Consejo Nacional de Seguridad] se llegó a la conclusión de que la amenaza a las tropas sobre el terreno era mayor que el valor de la inteligencia obtenida mediante la monitorización del sitio web, y un equipo especializado en redes informáticas [del Grupo Conjunto de Tareas — Operaciones de la Red Global] finalmente lo desmanteló¹³².

Como se ve en el ejemplo anterior, la coordinación entre distintos organismos es un factor importante para responder con éxito a las amenazas descubiertas.

229. Otros Estados Miembros, como el Reino Unido, han indicado que se ha hecho especial hincapié en el desarrollo de relaciones de trabajo y la concertación de memorandos de entendimiento entre el ministerio público y los organismos encargados de hacer cumplir la ley o los servicios de inteligencia, con resultados positivos. Asimismo, en Colombia, el Centro Integrado de Inteligencia e Investigación, o CI3, es el organismo nacional que coordina las investigaciones de presuntas actividades terroristas mediante una estrategia que descansa en seis pilares. En este sistema, la dirección y el mando generales de las diferentes fases de la investigación, que incluyen la reunión, la verificación y el análisis de las pruebas, están a cargo de un oficial superior de la policía nacional; en la fase judicial, la policía recoge información sobre las partes y los lugares asociados con la comisión de cualquier delito¹³³.

230. El experto de Francia describió el sistema nacional de coordinación de las respuestas de distintos organismos a las amenazas descubiertas:

- Fase 1: Los servicios de vigilancia e inteligencia detectan una amenaza mediante la monitorización de actividades en Internet.
- Fase 2: Los servicios de vigilancia notifican al ministerio público la amenaza detectada. El juez o el fiscal puede autorizar entonces a las autoridades policiales a poner bajo vigilancia la actividad en Internet del sospechoso descubierto. A partir de 2011, la legislación permite al juez de instrucción autorizar a la policía a registrar los datos informáticos de la persona monitorizada. Además, se puede solicitar a los proveedores de los servicios pertinentes que proporcionen los datos personales (por ejemplo, nombre, número de teléfono, número de tarjeta de crédito).
- Fase 3: Se lleva a cabo la investigación sobre la base de la información reunida a partir de las fuentes indicadas en las fases 1 y 2.

¹³²Ibid, pág. 13.

¹³³Oficina de las Naciones Unidas contra la Droga y el Delito, *Compendio de casos relativos a la lucha contra el terrorismo*, párr. 191.

G. Formación

231. Los funcionarios encargados de hacer cumplir la ley que investigan el uso de Internet con fines terroristas necesitan una formación especializada en los aspectos técnicos de los métodos seguidos por los terroristas y otros delincuentes para poner Internet al servicio de sus fines ilícitos, y en la forma en que los investigadores pueden servirse eficazmente de Internet para monitorizar las actividades de los grupos terroristas. La formación puede impartirse a través de iniciativas del sector público o privado, o una combinación de ambas.

232. Organismos como Europol o INTERPOL pueden dictar cursos sobre la ciencia forense de la tecnología de la información y la investigación de la ciberdelincuencia a nivel regional o internacional. Además, varios países han desarrollado sus propios programas de capacitación del personal policial en ciberdelincuencia, ya sea solos o en colaboración con instituciones académicas. También se puede impartir formación mediante cursos de capacitación *ad hoc*, seminarios, conferencias y capacitación práctica organizados por el sector público o las partes interesadas del sector económico afectado.

233. También pueden impartir formación especializada las instituciones académicas, como la Universidad de Dublín, en Irlanda, que en 2006 creó el Centro de Investigación sobre la Seguridad y la Delincuencia Cibernéticas. Los programas ofrecidos por la Universidad incluyen la maestría en informática forense e investigación de la ciberdelincuencia para personal policial. Otros cursos también ofrecen formación a los socorristas o equipos de respuesta inicial para apoyar su función operacional en relación con los casos de ciberdelincuencia.

234. Los Centros sobre ciberdelincuencia de la Red de Excelencia para la Capacitación, Investigación y Educación (2CENTRE) son un proyecto financiado por la Comisión Europea que se inició en 2010 con el objetivo de crear una red de Centros sobre ciberdelincuencia de excelencia para la capacitación, investigación y educación en Europa. Actualmente se están estableciendo centros en Bélgica, Estonia, Francia e Irlanda. Cada centro nacional se basa en una alianza entre los representantes de la fuerza pública, el sector privado y el mundo académico, que colaboran para desarrollar programas pertinentes de formación y cualificación, así como herramientas para su uso en la lucha contra la ciberdelincuencia. El Centro de Investigación sobre la Seguridad y la Delincuencia Cibernéticas de la Universidad de Dublín dirige y coordina el proyecto¹³⁴.

235. También se puede obtener formación en línea para la lucha contra el terrorismo, gracias a la Plataforma de capacitación y de cooperación en línea contra el terrorismo, de la UNODC, que se inició en 2011¹³⁵. La plataforma es una herramienta interactiva diseñada específicamente para capacitar a los profesionales de la justicia penal en la

¹³⁴ Véase www.2centre.eu.

¹³⁵ Véase <http://www.unodc.org/unodc/es/terrorism/unodc-counter-terrorism-learning-platform.html>.

lucha contra el terrorismo, al tiempo que los introduce en una comunidad virtual única donde pueden compartir sus experiencias e ideas respecto de la lucha antiterrorista. Además de permitir a los profesionales que han participado anteriormente en la capacitación proporcionada por la UNODC conectarse y crear redes con sus homólogos, la plataforma los mantiene al tanto de las novedades jurídicas en la materia, los informa acerca de las próximas oportunidades de formación y los induce a participar en actividades de aprendizaje permanente.

V. Cooperación internacional

A. Introducción

236. La velocidad, el alcance global y el anonimato relativo que ofrece Internet a los terroristas para promover sus causas o facilitar sus atentados, sumados a complejas cuestiones relacionadas con la ubicación, retención, incautación y presentación de los datos relacionados con Internet, hacen que la cooperación internacional eficaz y oportuna entre los organismos encargados de hacer cumplir la ley y los servicios de inteligencia sea un factor cada vez más importante para el éxito de la investigación y el enjuiciamiento de muchos casos de terrorismo.

B. Instrumentos y acuerdos de cooperación internacional

1. Instrumentos universales de lucha contra el terrorismo

237. Los instrumentos universales de lucha contra el terrorismo, es decir, las convenciones y los protocolos internacionales y las resoluciones pertinentes del Consejo de Seguridad, contienen mecanismos amplios para la cooperación internacional en los procesos penales relacionados con el terrorismo. Estos instrumentos prevén la extradición, la asistencia judicial recíproca, la remisión de actuaciones penales y el traslado de las personas condenadas, la ejecución recíproca de sentencias, el embargo preventivo y decomiso de activos y el intercambio de información entre los organismos encargados de hacer cumplir la ley.

238. Los elementos clave de los instrumentos contra el terrorismo relacionados con la cooperación internacional son:

- La obligación de llevar a los autores de actos de terrorismo a la justicia
- La obligación de extraditar o juzgar (principio *aut dedere aut judicare*)
- La obligación de establecer la competencia jurídica en ciertas circunstancias
- La obligación de excluir la excepción de los delitos políticos como motivo para rechazar una solicitud de cooperación
- Respeto por el estado de derecho y los derechos humanos
- Respeto por el principio de la doble incriminación
- Respeto por el principio de la especialidad

- Respeto por el principio *ne bis in idem* (cosa juzgada): prohibición de un segundo juicio por el mismo delito¹³⁶.

239. Los principios generales aplicables a la extradición y la asistencia judicial recíproca en los casos de terrorismo o de delincuencia organizada transnacional son parte de los mecanismos amplios establecidos en los instrumentos universales contra el terrorismo y otros instrumentos relativos a la delincuencia organizada transnacional (por ejemplo, la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional)¹³⁷. No es la intención de la presente publicación proporcionar una actualización o análisis detallados de cómo deben ser aplicados estos principios por los Estados a nivel nacional. Más bien, el interés se centra en determinar, dentro del amplio marco de cooperación internacional derivado de estos instrumentos, y con referencia a los principios y mecanismos establecidos, cuáles son las características concretas de los casos de terrorismo en que se usa Internet, con el fin de orientar a los encargados de formular políticas y a los profesionales de la justicia en cuanto a los enfoques o las estrategias que reflejan las buenas prácticas actuales.

a) *Ausencia de un instrumento universal relativo a cuestiones cibernéticas*

240. Si bien es probable que los mecanismos de cooperación internacional previstos en los instrumentos universales contra el terrorismo, de aplicarse plenamente, proporcionen una base jurídica para la cooperación en muchos casos de actos cometidos por medio de Internet por personas implicadas en una conducta ilícita tipificada en esos instrumentos, ninguno de ellos trata específicamente de actos relacionados con Internet en sí mismos. A falta de un instrumento contra el terrorismo que se ocupe específicamente de las cuestiones de Internet relacionadas con el terrorismo, las autoridades, cuando investigan y persiguen estos casos, seguirán recurriendo a los tratados o acuerdos internacionales o regionales vigentes, establecidos para facilitar la cooperación internacional en la investigación y persecución de actos de terrorismo o de la delincuencia organizada transnacional en general.

241. Es evidente que la cooperación internacional en la investigación y persecución de los casos de terrorismo relacionados con el uso de Internet por los terroristas se ve dificultada, en cierta medida, por la ausencia de un instrumento universal que trate específicamente de cuestiones cibernéticas. Sin embargo, no es el propósito del presente documento evaluar los méritos relativos de los argumentos en favor o en contra de la utilidad de elaborar un instrumento universal amplio que tratara, entre otras cosas, de la cooperación internacional en asuntos penales (incluido el terrorismo) relacionados con cuestiones cibernéticas. Su principal propósito es, más bien, determinar qué elementos, en el actual marco internacional, representan obstáculos para la cooperación y cómo pueden ser utilizados los instrumentos y acuerdos existentes por las autoridades nacionales para facilitar o fortalecer la cooperación internacional en los casos de terrorismo relacionados con algún aspecto del uso de Internet.

¹³⁶Oficina de las Naciones Unidas contra la Droga y el Delito, *Manual sobre cooperación internacional en asuntos penales relacionados con la lucha contra el terrorismo* (2009), secc. 1. C.

¹³⁷Naciones Unidas, *Treaty Series*, vol. 2225, núm. 39574.

b) *Otros instrumentos: la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y el Convenio sobre el delito cibernético del Consejo de Europa*

242. La Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional es el principal instrumento internacional que trata de la cooperación internacional entre los Estados en relación con los casos graves de delincuencia organizada transnacional. Los artículos 16 (extradición), 18 (asistencia judicial recíproca), 19 (investigaciones conjuntas) y 27 (cooperación en materia de cumplimiento de la ley) de la Convención tratan de la cooperación internacional. Aunque la conducta ilícita que menciona la Convención se refiere a la delincuencia organizada transnacional, no al terrorismo, los principios y mecanismos básicos de la Convención relativos a la cooperación internacional son muy similares a los que figuran en los instrumentos universales contra el terrorismo. Por consiguiente, los Estados Partes que han cumplido sus obligaciones de cooperación internacional en virtud de estos instrumentos deberían tener marcos y mecanismos ampliamente compatibles.

243. Además del Convenio sobre el delito cibernético del Consejo de Europa, el Convenio Europeo para la Prevención del Terrorismo, del Consejo de Europa¹³⁸; el Convenio europeo sobre extradición, con sus tres protocolos adicionales¹³⁹; el Convenio europeo sobre cooperación judicial en materia penal¹⁴⁰, con sus dos protocolos adicionales¹⁴¹; y el Acto 2000/C 197/01 [de 29 de mayo de 2000] del Consejo de la Unión Europea, que establece, de conformidad con el artículo 34 del Tratado de la Unión Europea, el Convenio relativo a la asistencia judicial en materia penal entre los Estados miembros de la Unión Europea, podrían constituir una base jurídica para la cooperación internacional en los casos de terrorismo que entrañen algún elemento de uso de Internet.

244. El Convenio sobre el delito cibernético del Consejo de Europa contiene disposiciones destinadas a fomentar la cooperación internacional mediante los mecanismos de cooperación policial y judicial y las medidas provisionales en caso de urgencia, por ejemplo, la comunicación oficiosa de información espontánea previa solicitud (art. 26) y el establecimiento de contactos disponibles a toda hora (art. 35). Estas solicitudes pueden ir acompañadas de una solicitud de no divulgación y proporcionar un mecanismo jurídico que permita el uso de medios oficiosos de comunicación y de intercambio de información entre las partes en la Convención, incluso si no tienen ninguna disposición de ese tipo en su legislación nacional.

245. Cabe señalar que el Convenio sobre el delito cibernético del Consejo de Europa está abierto no solo a los miembros del Consejo de Europa o de los Estados no miembros que hayan participado en su elaboración, sino también a otros Estados no miembros, que pueden adherirse al Convenio siempre que haya acuerdo unánime de los Estados contratantes con derecho a formar parte del Comité de Ministros.

¹³⁸ Consejo de Europa, *Serie de tratados europeos*, núm. 24.

¹³⁹ *Ibid.*, núms. 86, 98 y 209.

¹⁴⁰ *Ibid.*, núm. 30.

¹⁴¹ *Ibid.*, núms. 99 y 182.

2. Otros acuerdos regionales o multilaterales

246. Además de los instrumentos internacionales y regionales mencionados, los Estados pueden concertar tratados o acuerdos bilaterales o multilaterales que contengan disposiciones específicas sobre la cooperación en casos de actividades cibernéticas relacionadas con el terrorismo o la delincuencia transnacional. La extradición y la asistencia judicial recíproca tienden a estar reguladas por tratados o bien por “el derecho incipiente”, acordado por bloques de países. Sin embargo, las organizaciones regionales y subregionales también desempeñan un papel importante en la tarea de facilitar el intercambio de información y la cooperación en los arreglos mutuamente convenidos.

a) Orden de detención europea: marco de Schengen

247. La orden de detención europea en el marco de Schengen es un instrumento de cooperación aplicable en todos los Estados miembros de la Unión Europea, que ha demostrado ser extremadamente útil para el fortalecimiento de la cooperación judicial en la investigación y el enjuiciamiento de casos penales en Europa, incluidos los relacionados con el terrorismo. Una vez dictada la orden, las autoridades de otro Estado miembro están obligadas, sobre la base de la reciprocidad, a detener y trasladar a un delincuente, presunto o condenado, al Estado donde se dictó la orden, para que la persona pueda ser sometida a juicio o completar un período de detención. En este contexto, cabe señalar que la orden de detención europea establece, entre otras cosas, la extradición de los propios nacionales de un Estado miembro, concepto anteriormente ajeno a las disposiciones legislativas (incluso, a veces, constitucionales) de muchos Estados adheridos al llamado sistema continental europeo.

b) Exhorto europeo de obtención de pruebas

248. Desde que entró en vigor en 2009, el exhorto europeo ha ofrecido, de manera similar a la orden de detención europea con respecto a las detenciones, un procedimiento simplificado para la obtención y remisión de elementos de prueba, incluidos objetos, documentos y datos, entre los Estados miembros para su uso en actuaciones penales. A los efectos del exhorto europeo de obtención de pruebas, los datos reunidos pueden incluir datos de usuarios de Internet¹⁴².

249. Con el uso de estas decisiones marco y otros instrumentos internacionales, los Estados europeos han establecido, como bloque, un enfoque colectivo amplio y altamente desarrollado del problema de la obtención y remisión transfronterizas de pruebas y la extradición o entrega de delincuentes para su enjuiciamiento. Otros gobiernos podrían considerar, a nivel político y operacional, la conveniencia de adoptar, con los ajustes necesarios, un enfoque colectivo a nivel regional o subregional para armonizar sus esfuerzos de cooperación en la investigación y el enjuiciamiento transfronterizos de delitos de terrorismo.

¹⁴²Voislav Stojanovski, “The European evidence warrant”, en *Dny práva — 2009 — Days of Law: the Conference Proceedings*, 1a ed., David Sehnálek y colaboradores, eds. (Brno, República Checa, Universidad Masaryk, 2009).

c) *Planes del Commonwealth relativos a la extradición y a la asistencia judicial recíproca*

250. De manera similar a lo que ocurre con la orden de detención europea en el marco Schengen, el Plan de traslado de delincuentes convictos entre los países del Commonwealth (Plan de Londres) proporciona un mecanismo simplificado de extradición entre los países del Commonwealth, que prevé la detención provisional de los infractores, sobre la base de órdenes de detención dictadas por otros países miembros, sin necesidad de una evaluación de la suficiencia probatoria de los argumentos contra el sospechoso. El Plan define los delitos que permiten la extradición como aquellos que constituyen delitos en ambos países y se reprimen con una pena de prisión de dos años o más.

251. Del mismo modo, el Plan del Commonwealth para la Asistencia Mutua en Materia Penal (Plan de Harare) tiene por objeto aumentar el volumen y alcance de la asistencia prestada entre los países del Commonwealth en materia penal, facilitando la identificación y el paradero de las personas, la notificación de documentos, el examen de testigos, el registro y la incautación de pruebas, la comparecencia de testigos, el traslado temporal de personas detenidas para que presten testimonio, la entrega de documentos judiciales u oficiales, el rastreo, la incautación y el decomiso del producto o los instrumentos del delito, así como la conservación de datos informáticos.

252. Si bien los planes del Commonwealth no constituyen tratados propiamente dicho, son ejemplos de acuerdos no vinculantes, o “derecho incipiente”, con arreglo a los cuales algunos países se han comprometido a incorporar leyes compatibles en su legislación interna, de acuerdo con los principios acordados, para simplificar la extradición y la asistencia judicial recíproca entre ellos en causas penales, incluidas las investigaciones y persecuciones relacionadas con el terrorismo.

d) *Consejo de Europa*

253. Además de la elaboración de instrumentos encaminados a promover la cooperación internacional en causas penales relacionadas con la ciberdelincuencia, incluido el terrorismo, el Consejo de Europa también estableció (en virtud del artículo 35 del Convenio sobre el delito cibernético) la Red 24/7 de contactos disponibles las 24 horas del día, los siete días de la semana, que tiene por objeto facilitar la cooperación internacional en casos de ciberdelincuencia. Los proyectos regionales CyberCrime@IPA y Cybercrime@EAP, entre otros, del Consejo de Europa y la Unión Europea, apoyan la participación de los contactos 24/7 en cursos de capacitación, lo que les brinda la oportunidad de vincularse entre sí y de comunicarse con miembros de la red del Grupo de los Ocho (G-8).

254. Desde 2006, el Consejo de Europa viene apoyando, con su Proyecto Global sobre la Ciberdelincuencia, a los países de todo el mundo en las tareas de fortalecer la legislación; capacitar a los jueces, fiscales e investigadores encargados de hacer cumplir la ley en los asuntos relacionados con la ciberdelincuencia y las pruebas electrónicas, y de facilitar la cooperación internacional entre las fuerzas del orden y los proveedores

de servicios¹⁴³. Desde 2010, un tema de particular interés ha sido la investigación de las actividades financieras y corrientes de dinero delictivas en Internet, incluida la financiación del terrorismo basada en Internet¹⁴⁴.

e) *Plan de acción de la Unión Europea: centro de ciberdelincuencia*

255. El 26 de abril de 2010, reconociendo el papel fundamental que desempeña la tecnología de la información y las comunicaciones en la sociedad moderna y el número, alcance, complejidad y posible impacto cada vez mayores de las amenazas de la ciberdelincuencia para múltiples Estados, lo cual subraya la necesidad de una cooperación más estrecha entre los Estados miembros y el sector privado, el Consejo de la Unión Europea adoptó una serie de conclusiones sobre un plan de acción para la ciberdelincuencia, que se incluirán en el Programa de Estocolmo para el período 2010-2014 y la correspondiente futura Estrategia de Seguridad Interior.

256. En virtud del plan, los miembros acordaron, entre otras cosas, otorgar a la Comisión Europea el mandato de analizar, e informar al respecto, en cooperación con Europol, la utilidad y viabilidad de establecer un centro europeo de la ciberdelincuencia para reforzar los conocimientos, la capacidad y la cooperación en cuestiones relacionadas con los delitos cibernéticos. Concluida esta tarea, se ha formulado una propuesta de que la Europol acoja un nuevo servicio para la recepción y el procesamiento de los ficheros de análisis relacionados con la delincuencia organizada grave y el terrorismo.

3. *Función de otras organizaciones y acuerdos de cooperación regionales*

257. Como ya se indicó, los acuerdos oficiales de cooperación, a nivel regional o subregional, entre los organismos encargados de hacer cumplir la ley y los servicios de inteligencia desempeñan un papel fundamental en los esfuerzos de la comunidad internacional por fortalecer y coordinar las medidas dirigidas contra el terrorismo y la delincuencia organizada transnacional. Si bien la cooperación en virtud de estos acuerdos generalmente no se basa en tratados u otros instrumentos jurídicamente vinculantes, puede proporcionar mecanismos muy eficaces para la cooperación entre los países miembros participantes.

258. A nivel internacional, hay muchos ejemplos de tales acuerdos, pero tres de ellos, aplicables en Europa, África y el Pacífico, ilustran cómo los grupos de países con intereses y objetivos compatibles en cuanto a la ejecución de la ley y la seguridad pueden colaborar con éxito para desarrollar y armonizar una cooperación estrecha en las investigaciones penales.

¹⁴³Véase www.coe.int/lportal/web/coe-portal/what-we-do/rule-of-law/terrorism.

¹⁴⁴Consejo de Europa, Comité Especial de Expertos sobre la evaluación de medidas contra el blanqueo de dinero y la financiación del terrorismo, *Criminal Money Flows on the Internet: Methods, Trends and Multi-Stakeholder Counteraction* (2012).

259. El Centro franco-alemán de cooperación policial y aduanera, conocido también por el nombre de Centro Offenburg, se estableció en 1998, entre otras cosas, para prestar apoyo a la coordinación de las operaciones de varios organismos (por ejemplo, las operaciones de registro y vigilancia y el intercambio de la información obtenida) a través de la frontera común de esos países. Su personal está integrado por personal de la policía y de aduanas, así como de los organismos de seguridad de las fronteras, tanto a nivel federal como estatal, y tramita varios miles de solicitudes por año, y, al tiempo que sirve de plataforma para mediar soluciones pragmáticas a los problemas planteados entre organismos asociados, fomenta la confianza y la cooperación entre los distintos organismos.

260. En África, los miembros de la Organización Coordinadora de Jefes de Policía del África Meridional y de la Organización de Cooperación de los Jefes de Policía del África Oriental se han puesto de acuerdo respecto de las esferas específicas en que los organismos policiales han de cooperar, en particular en el intercambio periódico de información relacionada con la delincuencia; la planificación, coordinación y ejecución de operaciones conjuntas, incluidas las operaciones encubiertas; el control de las fronteras y la prevención de la delincuencia en las zonas fronterizas, así como en las operaciones de seguimiento; la entrega controlada de sustancias ilegales o de cualquier otro objeto, y la asistencia técnica y de expertos, en caso necesario¹⁴⁵.

261. En la región del Pacífico, el Centro de Coordinación de la Lucha contra la Delincuencia Transnacional en la Región del Pacífico ofrece una base para la reunión, la coordinación, el análisis y el intercambio de los datos de inteligencia criminal recogidos a través de una red de dependencias nacionales sobre delincuencia transnacional ubicadas en países miembros de la región. El Centro, cuyo personal está integrado por funcionarios adscritos de organismos encargados de hacer cumplir la ley y organismos de fronteras de los países insulares del Pacífico, ofrece a los países miembros un punto de acceso a INTERPOL y otros organismos encargados de hacer cumplir la ley de todo el mundo, a través de la red internacional de la Policía Federal de Australia, que apoya la iniciativa.

262. Del mismo modo, los países que no están necesariamente cerca geográficamente, pero que tienen intereses comunes en esferas temáticas relacionadas con la ejecución de la ley y la seguridad, podrían celebrar acuerdos colectivos que permitiesen el intercambio de información y de inteligencia.

a) *Grupo Egmont de unidades de inteligencia financiera*

263. Un ejemplo de un acuerdo de ese tipo con implicaciones para las investigaciones relacionadas con la financiación del terrorismo es el Grupo Egmont de unidades de inteligencia financiera. Las investigaciones de la presunta financiación del terrorismo invariablemente entrañan la reunión, el intercambio y el análisis de documentos

¹⁴⁵ Charles Goredema, "Inter-State cooperation", en *African Commitments to Combating Organised Crime and Terrorism: A review of eight NEPAD countries* (Iniciativa Africana sobre Seguridad Humana, 2004). Puede consultarse en www.iss.co.za/pubs/Other/ahsi/Goredema_Botha/pt1chap5.pdf.

financieros o bancarios ubicados en una o más jurisdicciones. En estos casos, es probable que la capacidad de las unidades de inteligencia financiera de cooperar y compartir la inteligencia financiera sea decisiva para la investigación y el enjuiciamiento. El Grupo Egmont, organismo internacional creado en 1995, trabaja para promover y mejorar la cooperación entre las unidades de inteligencia financiera en un esfuerzo por combatir el blanqueo de dinero y la financiación del terrorismo y fomentar, entre otras cosas, la ampliación y sistematización de la cooperación internacional en el intercambio recíproco de información. El Grupo Egmont recomienda que sus miembros concierten memorandos de entendimiento por los que se comprometan a intercambiar la inteligencia financiera pertinente para la investigación y persecución de la financiación del terrorismo, el blanqueo de dinero y otras actividades delictivas conexas.

264. Con el fin de asegurarse de que sus unidades nacionales de inteligencia financiera sean capaces de cooperar eficazmente con sus homólogos extranjeros en tales casos, las autoridades deberían considerar la conveniencia de concertar acuerdos o arreglos apropiados de intercambio de información con sus homólogos extranjeros. El memorando de entendimiento modelo propuesto por el Grupo Egmont proporciona una guía útil sobre los tipos de problemas que puede resultar necesario abordar.

b) Organización Internacional de Policía Criminal

265. Muchos instrumentos internacionales, como el Convenio Internacional para la represión de la financiación del terrorismo¹⁴⁶ (art. 18, párr. 4) y la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional (art. 18, párr. 13) y distintas resoluciones del Consejo de Seguridad, incluida la resolución 1617 (2005), alientan expresamente a los países a que encuadren la cooperación para el intercambio de información en el marco de INTERPOL.

266. Una de las funciones esenciales de INTERPOL es promover la cooperación internacional entre los organismos internacionales de aplicación de la ley y el intercambio y análisis rápido y seguro de la información relacionada con actividades delictivas. Lleva a cabo esta tarea gracias a su sistema I-24/7, que está a disposición de los funcionarios encargados de hacer cumplir la ley de todos los países miembros.

267. Utilizando el sistema I-24/7, las oficinas centrales nacionales pueden buscar y cotejar una amplia gama de datos, por ejemplo, información sobre sospechosos de terrorismo, en distintas bases de datos. El objetivo del sistema es facilitar la realización de investigaciones penales más eficaces proporcionando una gama más amplia de información a los investigadores.

268. Además de la red I-24/7, el programa de ciberdelincuencia de INTERPOL tiene por objeto promover el intercambio de información entre los países miembros por conducto de los grupos de trabajo y las conferencias regionales; dictar cursos de capacitación para establecer y mantener normas profesionales; coordinar las operaciones

internacionales y prestarles asistencia; establecer una lista mundial de contactos para las investigaciones de delitos cibernéticos; asistir a los países miembros en caso de ataques cibernéticos y en sus investigaciones de delitos mediante servicios de investigación y de base de datos; desarrollar alianzas estratégicas con otras organizaciones internacionales y entidades del sector privado; detectar las amenazas nuevas y compartir esta información con los países miembros, así como proporcionar un portal web seguro para el acceso a la información y documentos operacionales¹⁴⁷.

269. Desde 2009, INTERPOL viene trabajando en estrecha colaboración con la Universidad de Dublín para ofrecer formación especializada e intercambios académicos a fin de promover los conocimientos especializados en la investigación de la ciberdelincuencia. En agosto de 2011, investigadores de la ciberdelincuencia y especialistas en investigación informática forense de 21 países tomaron parte en el primer curso de capacitación en ciberdelincuencia de la escuela de verano de INTERPOL y la Universidad de Dublín. El programa, de dos semanas de duración, fue preparado por la Universidad e incluía ejercicios de simulación de casos; estuvo a cargo de profesionales de la ejecución de la ley, de la Universidad de Dublín y el sector privado. El curso, que tenía por objeto desarrollar los conocimientos teóricos y prácticos, así como las técnicas pertinentes en una serie de esferas para ayudar a los investigadores a realizar investigaciones más eficaces de la ciberdelincuencia, capacitó a los participantes en el uso de técnicas tales como la obtención de imágenes de discos, análisis forense de datos en tiempo real, análisis forense de teléfonos móviles, investigaciones de blanqueo de dinero, técnicas de registro e incautación, investigaciones de comunicaciones VoIP e inalámbricas y detección y análisis de programas informáticos maliciosos¹⁴⁸.

270. Por último, la Unidad de INTERPOL sobre Delincuencia de Alta Tecnología facilita la cooperación operacional entre los países miembros mediante reuniones de grupos de expertos en delitos informáticos y cursos prácticos de capacitación, mundiales y regionales, así como la cooperación entre las autoridades policiales, el sector privado y los medios académicos. También ayuda a los países miembros en caso de ataque cibernético y en las investigaciones de ciberdelincuencia con sus servicios de investigación y de base de datos.

c) *Oficina Europea de Policía*

271. Una parte importante del mandato de la Europol consiste en aumentar la eficacia de las fuerzas del orden de los Estados miembros de la Unión Europea y estrechar la cooperación entre ellas para prevenir y combatir mejor el terrorismo y otras formas de delincuencia organizada transnacional. La Europol desempeña un papel fundamental en el Equipo de Tareas europeo sobre ciberdelincuencia, grupo de expertos integrado por representantes de la Europol, Eurojust y la Comisión Europea, que colabora con los jefes de las unidades de la Unión Europea sobre delitos informáticos para facilitar la lucha transfronteriza contra la ciberdelincuencia. La Europol ofrece el siguiente apoyo

¹⁴⁷ Véase www.interpol.int/Crime-areas/Cybercrime/Cybercrime.

¹⁴⁸ Ibid.

a los Estados miembros de la Unión Europea en cuestiones relacionadas con la ciberdelincuencia:

- Base de datos sobre ciberdelincuencia: la Europol proporciona a los Estados miembros de la Unión Europea apoyo investigativo y analítico sobre la ciberdelincuencia y facilita la cooperación y el intercambio de información transfronterizos
- El programa de evaluación de la amenaza de la delincuencia organizada facilitada por Internet (iOCTA) analiza las tendencias actuales y futuras de la ciberdelincuencia, incluidas las actividades terroristas y los ataques contra las redes electrónicas, y en esa información se fundan tanto las actividades operacionales como las políticas de la Unión Europea
- El Sistema de denuncias en línea de delitos cometidos por Internet (ICROS) y el Foro de Expertos Forenses (iFOREX) están actualmente en desarrollo. Estas dos iniciativas proporcionarán una coordinación centralizada de las denuncias de delitos cibernéticos procedentes de las autoridades de Estados miembros de la Unión Europea y, además de dar acogida a datos técnicos, organizarán cursos de capacitación para la policía¹⁴⁹.

272. Además de prestar este apoyo a nivel operacional y en colaboración con Eurojust, la Europol participa activamente en el establecimiento de equipos conjuntos de investigación, a los que ofrece ayuda, y asiste a los Estados miembros en sus investigaciones mediante ficheros de trabajo analítico y reuniones de coordinación y tácticas basadas en casos. En el marco de la plataforma de ficheros de trabajo analítico, almacena los datos nominativos (por ejemplo, información sobre testigos, víctimas, números de teléfono, lugares, vehículos y hechos) y los somete a un proceso dinámico de análisis que permite vincular objetos, entidades y datos entre las indagaciones y las investigaciones nacionales. Los datos se marcan con un “código de manejo” que indica claramente las condiciones de uso aplicables a dicho componente particular de los datos.

d) *Eurojust*

273. Como parte de su mandato, la labor de Eurojust en el ámbito de lucha contra el terrorismo incluye la facilitación del intercambio de información entre las autoridades judiciales de los distintos Estados miembros que llevan a cabo investigaciones y enjuiciamientos relacionados con el terrorismo¹⁵⁰; el apoyo a las autoridades judiciales de los Estados miembros en la emisión y ejecución de órdenes de detención europeas, y la facilitación de las medidas de investigación y obtención de pruebas necesarias para

¹⁴⁹ Véase “Cybercrime presents a major challenge for law enforcement”, comunicado de prensa de la Oficina Europea de Policía de 3 de enero de 2011. Puede consultarse en www.europol.europa.eu/content/press/cybercrime-presents-major-challenge-law-enforcement-523.

¹⁵⁰ La decisión 2005/671/JAI del Consejo de la Unión Europea, de 20 de septiembre de 2005, relativa al intercambio de información y a la cooperación sobre delitos de terrorismo obliga a todos los Estados miembros a designar correspondientes nacionales para los asuntos de terrorismo, que deben informar a Eurojust (la unidad de cooperación judicial de la Unión Europea) de todas las actividades terroristas en su país, desde las primeras etapas, en que se entrevista a los sospechosos, hasta la etapa de acusación, y desde la emisión de órdenes de detención europeas en relación con el terrorismo, hasta las solicitudes de asistencia judicial recíproca y las sentencias.

que los Estados miembros puedan perseguir los presuntos delitos de terrorismo (por ejemplo, testimonio de testigos, pruebas científicas, registros e incautaciones, y la interceptación de comunicaciones). Los 27 miembros nacionales de Eurojust (jueces, fiscales o autoridades policiales con competencias equivalentes en sus respectivos Estados miembros) tienen su base en La Haya (Países Bajos) y se mantienen en contacto permanente con las autoridades nacionales de sus respectivos Estados miembros, que pueden solicitar el apoyo de Eurojust en el curso de investigaciones o persecuciones particulares del terrorismo (por ejemplo, para resolver conflictos de competencia o facilitar la obtención de pruebas).

274. Eurojust también alienta y apoya la creación y la labor de los equipos conjuntos de investigación, proporcionando información y asesoramiento a los profesionales que los integran. Cada vez está más generalizada la opinión de que los equipos conjuntos de investigación son un instrumento eficaz en la respuesta judicial a la delincuencia transfronteriza y un foro adecuado donde intercambiar información operacional en ciertos casos de terrorismo. Los miembros nacionales de Eurojust pueden participar en equipos conjuntos de investigación, actuando en nombre de Eurojust o en su calidad de autoridades nacionales competentes en materia de terrorismo. Por ejemplo, en un caso danés relacionado con actividades terroristas, en que se envió a las autoridades belgas una solicitud para establecer un equipo conjunto de investigación, los representantes danés y belga de Eurojust participaron en la creación del equipo de las dos autoridades nacionales competentes. Eurojust también proporciona asistencia financiera y logística a las operaciones de tales equipos y es sede de la secretaría permanente de los equipos conjuntos de investigación.

275. El *Terrorism Convictions Monitor* de Eurojust procura, entre otras cosas, proporcionar a los profesionales de la justicia ejemplos de sentencias en un país que podrían ser útiles en otro, en particular con respecto a la interpretación de la legislación de la Unión Europea contra el terrorismo. En su número de septiembre de 2010, el *Terrorism Convictions Monitor* presenta un análisis a fondo de dos casos con características comunes, a saber, el terrorismo relacionado con la yihad, la radicalización y el uso de Internet¹⁵¹. Uno de los casos, aportado por las autoridades belgas, era el de Malika el Aroud y otros, citado más adelante (véase el párrafo 377). El equipo de lucha contra el terrorismo de Eurojust organiza periódicamente reuniones tácticas y estratégicas sobre las tendencias del terrorismo, en las que destacados magistrados y expertos en derecho contra el terrorismo de países miembros y no miembros de la Unión Europea comparten sus conocimientos especializados sobre cuestiones concretas. Entre los ejemplos de tales reuniones cabe mencionar la reunión estratégica de 2010 relacionada con el uso de la tecnología VoIP con fines terroristas y la necesidad de interceptación legal, así como una reunión táctica celebrada en abril de 2011 sobre la violencia extremista o terrorista de causa única. En estas reuniones, se determinan cuáles son los problemas comunes y se difunden las conclusiones alcanzadas y las mejores prácticas entre las autoridades de la Unión Europea, al tiempo que se establecen los métodos adecuados para hacer más eficaz la coordinación de la lucha contra el terrorismo.

¹⁵¹El *Terrorism Convictions Monitor* puede obtenerse dirigiéndose al Eurojust Counter-Terrorism Team.

C. Marcos legislativos nacionales

276. La existencia, a nivel nacional, de un marco legislativo que prevea la cooperación internacional es un elemento fundamental de un marco eficaz para la facilitación de la cooperación internacional en la investigación y persecución de casos de terrorismo. Esta legislación debería incorporar en el derecho interno de un país los principios relacionados con la cooperación internacional consagrados en los instrumentos universales contra el terrorismo.

277. Además de editar una serie de publicaciones encaminadas a ayudar a los países a incorporar en su legislación nacional los mecanismos de cooperación internacional, la Subdivisión de Prevención del Terrorismo de la UNODC presta servicios de asesoramiento, capacitación y creación de capacidad en estas esferas como parte de su “menú” de servicios disponibles para los países en el cumplimiento de sus obligaciones internacionales contra el terrorismo.

D. Otras medidas fuera de las legislativas

278. Si bien la adhesión a instrumentos multilaterales y bilaterales y la adopción de la legislación correspondiente son componentes fundamentales de todo régimen eficaz de cooperación internacional, no constituyen la respuesta completa. Un elemento clave para el éxito de la prestación de una cooperación internacional eficaz es la presencia de una autoridad central, proactiva y dotada de recursos suficientes, capaz de facilitar, sobre la base de los mecanismos disponibles (oficiales y oficiosos), la cooperación de manera oportuna y eficiente.

279. Una condición importante para el éxito de la cooperación internacional es la existencia de una coordinación interinstitucional eficaz entre las autoridades policiales, los organismos de inteligencia especializados (por ejemplo, las unidades de inteligencia financiera) y las autoridades centrales a nivel nacional, con el apoyo de la legislación necesaria y procedimientos claros y simplificados para atender las solicitudes.

280. El caso que se presenta a continuación, juzgado en Colombia, con una amplia cooperación oficial y oficiosa entre las autoridades, es un buen ejemplo de cooperación a tanto nivel nacional como internacional.

Caso de las Fuerzas Armadas Revolucionarias de Colombia (FARC)

El 1 de marzo de 2008, las fuerzas armadas de Colombia llevaron a cabo varias operaciones contra presuntos miembros de las Fuerzas Armadas Revolucionarias de Colombia (FARC). Durante estas operaciones, se dio muerte a un individuo sospechoso de ser uno de los principales cabecillas de las FARC y a otros miembros de la organización, y se reunieron pruebas consistentes, entre otras cosas, en dispositivos electrónicos como computadoras, agendas digitales y memorias USB. Los objetos que contenían elementos de prueba digitales se pasaron a la policía judicial colombiana para su uso en posibles investigaciones y procesos penales.

Los datos obtenidos de los dispositivos digitales revelaron información relacionada con la red internacional de apoyo de la organización, que incluía enlaces con varios países de América Central y América del Sur y de Europa. El objetivo principal de esta red era la recaudación de fondos para las actividades de las FARC, el reclutamiento de nuevos miembros y la promoción de las políticas de la organización, incluida la eliminación de la designación de la organización como terrorista en diferentes listas mantenidas por la Unión Europea y algunos países. Basándose en las pruebas reunidas, la Procuraduría General de la Nación inició investigaciones penales de las personas que supuestamente prestaban apoyo y aportaban fondos a las FARC.

Las pruebas, que fueron compartidas por las autoridades colombianas con sus homólogos de España, llevaron a la identificación del cabecilla de las FARC en España, conocido por el alias de "Leonardo". "Leonardo" había entrado en España en 2000, y se le había concedido asilo político.

La Procuraduría General de la Nación obtuvo pruebas suficientes para pedir que se dictara una orden de detención con fines de extradición de "Leonardo" y recurrió a canales diplomáticos y otras vías jurídicas de cooperación internacional para solicitar su extradición a Colombia para ser juzgado.

"Leonardo" fue detenido en España y los registros de su domicilio y lugar de trabajo revelaron la existencia de documentos y dispositivos electrónicos que contenían pruebas de sus vínculos con los delitos investigados. Posteriormente fue puesto en libertad bajo fianza; su condición de refugiado impidió su extradición inmediata.

El proceso penal se inició en Colombia en contra de "Leonardo" en rebeldía por su supuesta participación en la financiación del terrorismo. En una decisión de la Corte Suprema de Justicia de Colombia, se consideró inadmisibles la información obtenida durante la operación de 1 de marzo de 2008 que se encontraba en los dispositivos electrónicos incautados. Posteriormente, el fiscal, junto con sus homólogos de otros países, donde se encontraban miembros de la red de apoyo a las FARC, recurrió a todos los canales disponibles de cooperación internacional para identificar a los miembros de la red en España y otros países europeos y reunir más pruebas en apoyo del caso.

Además, en respuesta a la comisión rogatoria emitida por la Procuraduría General de Colombia, las autoridades judiciales españolas transmitieron a sus homólogos colombianos toda la información recogida durante las redadas y registros del domicilio de "Leonardo". Según la policía judicial española, esta información establecía la culpabilidad de "Leonardo" y de otras personas con respecto a la formación de una célula terrorista de las FARC en España. También ayudó a establecer la culpabilidad de "Leonardo" por la financiación del terrorismo y reforzó la hipótesis de que probablemente existían vínculos entre "Leonardo" y personas sometidas a juicio por sus vínculos con el grupo terrorista Euskadi Ta Askatasuna (ETA) (Patria Vasca y Libertad). Los registros realizados en España dieron lugar a la incautación de más pruebas documentales y digitales, que eran sustancialmente similares a las que se habían declarado inadmisibles. Con estas nuevas pruebas proporcionadas por las autoridades españolas, la Procuraduría General siguió el proceso contra "Leonardo". Por otra parte, las nuevas pruebas revelaron los esfuerzos de las FARC por proporcionar a sus miembros acceso a las universidades, organizaciones no gubernamentales y otras entidades del Estado donde podían buscar oportunidades de financiación y reclutar nuevos miembros.

Las pruebas también confirmaron la existencia de una "comisión internacional" dentro de las FARC, que mantenía un programa de seguridad para las comunicaciones, en particular las transmitidas por Internet o por radio (medio permanente de comunicación entre los

cabecillas de la organización y los miembros de la red internacional de apoyo), mediante el cual cifraba la información transmitida, usando la esteganografía para ocultar mensajes, enviando mensajes electrónicos no solicitados y eliminando el historial de navegación para asegurarse de que la información no pudiera ser recuperada por las autoridades investigadoras o judiciales. En este sentido, las autoridades españolas y colombianas colaboraron para “quebrar” las claves y descifrar el contenido de los mensajes que se transmitían los presuntos cabecillas de las FARC en Colombia y España.

Antes de iniciar el procedimiento contra “Leonardo”, la Procuraduría General de la Nación presentó una solicitud a un juez de que las nuevas pruebas se considerasen “pruebas sobrevinientes” y de una “fuente independiente”. El objeto de esta solicitud, que fue concedida, era permitir la inclusión de las pruebas en las actuaciones judiciales sin activar los motivos que, de lo contrario, habrían llevado a la exclusión de pruebas similares.

El juicio del acusado “Leonardo” en rebeldía por cargos de financiación del terrorismo está actualmente en curso en Colombia, a la espera del resultado del trámite de extradición.

281. En el caso anterior, las autoridades aprovecharon tanto los mecanismos oficiales de asistencia judicial recíproca como los oficiosos. Aunque puede haber diferencias en el grado en que las autoridades de diferentes países pueden ayudarse mutuamente en ausencia de un tratado o una solicitud oficial, las autoridades tienen, en muchos países, cierta capacidad para prestar asistencia en respuesta a solicitudes oficiosas de sus homólogos extranjeros en investigaciones relacionadas con el terrorismo. En la reunión del grupo de expertos se destacaron varios casos y circunstancias en que se había recurrido o podría haberse recurrido a dicha cooperación oficiosa para investigar con éxito algunos casos relacionados con el uso de Internet por los terroristas.

1. Importancia de la confianza mutua

282. A nivel operacional, también es sumamente importante que los organismos nacionales encargados de hacer cumplir la ley y los representantes del ministerio público promuevan, establezcan y mantengan relaciones de confianza mutua con los homólogos extranjeros con quienes podrían tener necesidad de cooperar en investigaciones penales transfronterizas.

283. En vista de la naturaleza transnacional de gran parte del terrorismo y de las actividades delictivas conexas, el carácter sumamente complejo y delicado de las investigaciones basadas en datos de inteligencia, y la necesidad de proceder con celeridad cuando los acontecimientos y las investigaciones cambian de un momento a otro, la confianza entre los organismos policiales y fiscales, a nivel tanto nacional como internacional, suele ser un factor decisivo para el éxito de la investigación y persecución de delitos relacionados con el terrorismo. Esto es particularmente importante en el contexto de Internet, donde, por ejemplo, la conservación de datos de uso y las pruebas digitales almacenadas en computadoras y otros dispositivos portátiles, muchas veces en una o más jurisdicciones diferentes, suelen ser pruebas decisivas para el enjuiciamiento y tienen que obtenerse dentro de plazos perentorios. Los contactos personales con los homólogos de otras jurisdicciones, la familiaridad con sus procedimientos y la confianza son todos factores que contribuyen a la cooperación internacional eficaz.

284. Mientras que ciertos países pueden diferir en los medios con que prestan cooperación oficiosa, se pueden reconocer algunos elementos de buenas prácticas en la prestación de asistencia oficiosa en investigaciones relacionadas con el terrorismo.

a) *Desarrollo de mecanismos eficaces de intercambio de información: el uso de oficiales de enlace*

285. Varios participantes en la reunión del grupo de expertos observaron que los organismos nacionales encargados de hacer cumplir la ley tienen una red internacional de puestos de enlace que facilita en gran medida el trámite de las solicitudes de cooperación internacional. Por ejemplo, la Oficina de la Policía Criminal Federal de Alemania, la Bundeskriminalamt, cuenta con un oficial de enlace y con contactos directos en unos 150 países. Además, la Red de expertos europeos sobre cuestiones relacionadas con el terrorismo, establecida en 2007, reúne a expertos del mundo académico, la policía y los servicios de inteligencia y ha demostrado ser un canal muy eficaz para compartir información y conocimientos especializados sobre una base multidisciplinaria.

286. El caso de *R. c. Namouh* es un ejemplo de cooperación internacional de notable éxito que se llevó a cabo enteramente a título oficioso, entre las autoridades encargadas de hacer cumplir la ley o las fiscalías de Austria y el Canadá, en la investigación y el enjuiciamiento de personas que se encontraban en esas jurisdicciones y que usaban Internet para desarrollar actividades relacionadas con el terrorismo.

R. c. Said Namouh

El Sr. Said Namouh, nacional marroquí, vivía en un pequeño pueblo del Canadá.

El 10 de marzo de 2007, se publicó en un sitio web de Internet un video en la forma de carta "abierta", leída por el jeque Ayman al-Zawahiri. En ella, Al-Zawahiri advertía a los Gobiernos de Alemania y Austria que si no retiraban sus tropas de las misiones de apoyo a la paz en el Afganistán tendrían que atenerse a las consecuencias. En un pasaje de la declaración, Al-Zawahiri decía:

La paz es una cuestión recíproca. Si nosotros estamos a salvo, ustedes estarán a salvo. Si nosotros tenemos paz, ustedes tendrán paz, y si nos van a matar, ustedes, Dios mediante, serán vencidos y muertos. Se trata de una ecuación exacta. Traten, entonces, de entenderlo, si es que entienden.

El video, con las declaraciones adjuntas de Al-Zawahiri, se enmarcaba en un mosaico de imágenes que incluían vehículos blindados con banderas nacionales y prominentes políticos de Alemania y Austria. En algunas partes del video, había fotos de Al-Zawahiri y otras figuras encapuchadas.

Tras la difusión del video, las autoridades austríacas iniciaron una investigación que incluyó escuchas telefónicas de diversas comunicaciones de Mohammed Mahmoud, nacional austríaco que vivía en Viena. Estas comunicaciones, en árabe, consistían en sesiones de charla VoIP y de Internet que revelaban que el Sr. Mahmoud tenía comunicaciones con una persona residente en el Canadá sobre cuestiones relacionadas con la yihad, que incluían planes para realizar un atentado terrorista, muy probablemente en Europa. En sus comunicaciones, los participantes discutían el uso de explosivos y otras maneras de llevar a cabo el atentado.

Como resultado de las actividades de interceptación, se identificó a Said Namouh, que vivía en el Canadá, como uno de los participantes en las mencionadas comunicaciones. En julio de 2007, la Real Policía Montada del Canadá participó en la investigación, que coordinaban las autoridades austríacas y canadienses a través del enlace oficial de las fuerzas del orden del Canadá con sede en Viena. Aunque existía un tratado oficial de asistencia judicial recíproca entre Austria y el Canadá, no se presentó ninguna solicitud oficial de asistencia judicial recíproca con arreglo al tratado; la cooperación se llevó a cabo enteramente a título oficioso.

Las investigaciones revelaron que entre noviembre de 2006 y septiembre de 2007 alguien que utilizaba la conexión de Internet del Sr. Namouh pasaba una cantidad considerable de tiempo conectado, y se mantenía en contacto permanente con yihadistas de todo el mundo, incluso mediante el Frente Mundial de Medios de Información Islámicos (GIMF), uno de los grupos yihadistas virtuales más antiguos y prominentes. Apoyado por el Centro Al-Fajr, el Frente actúa como el brazo de prensa del Ejército del Islam [Jaish al-Islam]. Entre otras cosas, el Frente difunde propaganda y proporciona a los yihadistas las herramientas (por ejemplo manuales de fabricación de bombas, programas informáticos de cifrado) para llevar a cabo la yihad. Gran parte de la actividad en Internet del Sr. Namouh incluía anuncios en diferentes foros de debate frecuentados por yihadistas.

En mayo de 2007, el periodista de la BBC Alan Johnston fue secuestrado en Gaza por el "ejército del Islam". El Frente publicó varios videos relacionados con el secuestro, pero cabe señalar en particular el video publicado el 9 de mayo de 2007, en que el Ejército del Islam se declaraba responsable del secuestro, así como los videos publicados los días 20 y 25 de junio, en los que se hacían amenazas de ejecutarlo si no se cumplían ciertas exigencias. Afortunadamente, el Sr. Johnston fue liberado ileso el 3 de julio de 2007.

El 7 y 8 de mayo, las comunicaciones del Sr. Namouh hechas en un foro de charla de Internet e interceptadas por las autoridades, revelaron que el Sr. Namouh había participado en las conversaciones relacionadas con el secuestro de Alan Johnson y, concretamente, en las relativas a la preparación del mensaje del Frente en que se declaraba responsable, y que fue transmitido unos momentos más tarde, el 9 de mayo. Según una transcripción de la charla de Internet del 8 de mayo, presentada como prueba en el juicio (y traducida del árabe al francés), el Sr. Namouh declaró: "Mi querido hermano Abou Obayada, quédate con nosotros en la línea; que Dios te colme de bienes para que puedas ver lo que hay que hacer; la declaración se hará hoy, Dios mediante".

Entre el 3 de junio y el 9 de septiembre de 2007, Namouh y Mahmoud tuvieron 31 conversaciones en total. Estas conversaciones revelaron que proyectaban llevar a cabo un atentado con bomba en un lugar desconocido de Europa y discutían cómo obtener o hacer cinturones explosivos para ataques suicidas, cuestiones de financiación y planes para encontrarse con otras personas en el Magreb y Egipto para ultimar los preparativos. Estas conversaciones sugerían que el Sr. Namouh sería el autor del atentado suicida.

El 12 de septiembre de 2007, temiendo que los planes estuvieran a punto de consumarse, las autoridades de Austria y del Canadá llevaron a cabo simultáneamente las detenciones de Namouh y Mahmoud.

En el Canadá, el Sr. Namouh fue acusado de confabulación para utilizar explosivos (en un lugar desconocido de Europa), participación en las actividades de un grupo terrorista, facilitación de actividades terroristas y extorsión de un gobierno extranjero (video con amenazas contra Alemania y Austria).

En el juicio, la defensa del Sr. Namouh cuestionó varios aspectos de los argumentos de la fiscalía, aduciendo, entre otras cosas, argumentos constitucionales basados en el derecho a la libertad de expresión (relacionados con la cuestión de si el Frente era una organización terrorista). Se plantearon objeciones en cuanto a la objetividad del testigo pericial principal llamado por la fiscalía para prestar testimonio sobre el movimiento de Al-Qaida, sus facciones, el yihadismo mundial (incluido el yihadismo virtual) y los métodos y estilos de propaganda del Frente y el uso de Internet por la organización. La defensa también cuestionó la afirmación de que las actividades emprendidas por el Frente y grupos asociados constituyeran terrorismo, así como la fiabilidad de las pruebas relacionadas con la interceptación de comunicaciones por Internet en Austria y el Canadá y la exactitud de la traducción de las constancias de esas comunicaciones del árabe al francés. La defensa pidió al tribunal que determinara que los distintos mensajes distribuidos por el Sr. Namouh en nombre del Frente debían interpretarse en sentido figurado y no como actos que tuvieran el fin de aconsejar o alentar la comisión de actos terroristas.

Al examinar los argumentos de la defensa en relación con la naturaleza del material publicado o comunicado en nombre del Frente, el tribunal concluyó:

El tribunal no tiene ninguna duda al respecto. El contexto de estos mensajes se refiere claramente a actos reales alentados por el Frente. La muerte y destrucción están por todas partes. La yihad que promueve el Frente es de carácter violento. Esta promoción constituye claramente una forma de aliento y, a veces, una amenaza de actividades terroristas. Por tanto, esta actividad encuadra claramente en la definición de actividades terroristas conforme al artículo 83.01 del Código Penal.

Al declarar al Sr. Namouh culpable de aconsejar o alentar la comisión de actos de terrorismo, el tribunal citó las comunicaciones interceptadas, que contenían declaraciones que demostraban el carácter activo y entusiasta de su participación en las actividades del Frente. A juicio del tribunal, también eran importantes varios anuncios, incluido el del 12 de diciembre de 2006, que figura a continuación, en que el acusado expresaba su deseo de ocultar sus actividades y las del Frente eliminando datos informáticos incriminatorios:

[TRADUCCIÓN]

Urgente Urgente Urgente

La paz, la misericordia y las bendiciones de Dios sean con vosotros.

Quiero borrar todas las películas y los libros yihadistas que se encuentran en mi computadora sin dejar ningún rastro, que Dios os bendiga, porque me temo que alguien ha inspeccionado mi computadora.

Que la paz, la misericordia y las bendiciones de Dios sean con vosotros.

En otras comunicaciones, el acusado había hecho averiguaciones sobre el uso de programas informáticos de anonimato y herramientas similares que pudieran servir para ocultar sus actividades. Tras el juicio, en octubre de 2009, el acusado fue declarado culpable de todos los cargos; más tarde fue condenado a cadena perpetua.

b) *Investigaciones conjuntas*

287. Aunque el concepto de “investigaciones conjuntas” se menciona en algunos tratados internacionales (por ejemplo, el artículo 19 de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional), no existe ninguna referencia expresa a esta estrategia en los instrumentos universales contra el terrorismo. Sin embargo, este enfoque de las investigaciones está en perfecta consonancia con los

principios y el espíritu subyacentes de los elementos de cooperación internacional de estos instrumentos. Algunos países, particularmente en Europa, han adoptado con éxito este enfoque en una serie de investigaciones relacionadas con el terrorismo; cabe destacar, a este respecto, el importante papel de la Europol en la creación de equipos conjuntos de investigación y en el apoyo que reciben. El objetivo principal de estos equipos conjuntos de investigación, integrados tanto por funcionarios nacionales encargados de hacer cumplir la ley como por agentes de la Europol, es llevar a cabo investigaciones, con un propósito específico y de duración limitada, en uno o más de los Estados miembros¹⁵².

288. La Europol cuenta con un sistema de unidades nacionales, que son contactos designados dentro de las fuerzas policiales nacionales. Esto facilita y fomenta el intercambio de información entre los Estados miembros por medio de una red digital segura y proporciona un sistema de 17 ficheros de trabajo analítico dentro del marco jurídico de la Europol, con el fin primordial de facilitar a las autoridades participantes una coordinación y cooperación plenas.

289. Aunque es difícil evaluar, a nivel internacional, la medida en que los países han colaborado de esta manera, las discusiones en la reunión del grupo de expertos destacaron la conciencia cada vez mayor, en las comunidades internacionales de la ejecución de la ley y de la seguridad, de que el carácter del terrorismo moderno y los *modi operandi* de los terroristas hacen de una estrecha cooperación en la investigación del terrorismo un componente cada vez más importante del éxito de los esfuerzos para desbaratar, prevenir y perseguir los actos terroristas.

E. Cooperación oficial y oficiosa

290. La cooperación internacional en los casos de terrorismo que tienen un elemento transfronterizo puede asumir numerosas formas, según la naturaleza del delito que se esté investigando, el tipo de asistencia requerida, la legislación nacional aplicable y la existencia y el estado de cualquier tratado o acuerdo de apoyo.

291. Los procedimientos oficiales de asistencia judicial recíproca en asuntos penales, a pesar de las mejoras logradas en cuanto a su eficiencia y eficacia, pueden ser aún trámites largos, con mucho papeleo burocrático tanto en el país requirente como en el requerido. En muchos casos de terrorismo, sobre todo los de delitos relacionados con Internet, la cooperación oficiosa está demostrando ser, cada vez más, tan importante como los canales oficiales, por evitar demoras considerables en situaciones en que el tiempo es un factor crítico para tomar medidas (por ejemplo, para la conservación de datos sobre el uso de Internet) que son fundamentales para el éxito del enjuiciamiento. Los participantes en la reunión del grupo de expertos destacaron la importancia de que los servicios nacionales de inteligencia, las autoridades encargadas de hacer cumplir

¹⁵²Eveline R. Hertzberger, *Counter-Terrorism Intelligence Cooperation in the European Union* (Turín, Italia, Instituto Interregional de las Naciones Unidas para Investigaciones sobre la Delincuencia y la Justicia, julio de 2007).

la ley y el ministerio público desarrollaran y utilizaran de manera proactiva, siempre que fuera posible, los mecanismos disponibles para facilitar tanto los canales oficiales como los oficiosos de cooperación internacional.

292. En muchos casos, por ejemplo cuando las autoridades de un país buscan la conservación de datos de Internet en poder de los proveedores de servicios de Internet de otro país, las autoridades pueden cooperar oficiosamente para conservar esos datos con el fin de investigar o perseguir un delito penal.

293. Los problemas jurídicos que plantean las investigaciones penales relacionadas con Internet, especialmente los de competencia, pueden ser extremadamente complejos. En los casos en que los investigadores de un país necesitan acceder a la información almacenada en computadoras situadas en otro país, se pueden plantear cuestiones complejas respecto del fundamento de esas actividades y de la autoridad jurídica para llevarlas a cabo. Si bien es posible que las autoridades de un país puedan tratar directamente con las personas de otro país que tienen la información buscada, la reacción de estas últimas puede variar. Como norma general, es conveniente que las autoridades colaboren con sus homólogos extranjeros, de ser posible con carácter oficioso, para obtener dicha información.

294. La forma y el método de la cooperación dependerán en gran medida de la naturaleza y el propósito de la asistencia solicitada. Por ejemplo, si bien las autoridades de un país pueden prestar asistencia oficiosa a los homólogos extranjeros que busquen la conservación de datos de proveedores de servicios de Internet, el registro y la incautación de esos datos por lo general requieren autorización judicial, que solo puede obtenerse por medios oficiales.

295. A veces, la presentación de solicitudes oficiales es el único método por el que las autoridades pueden proporcionar la necesaria cooperación mutua. En esos casos, es importante que los países cuenten con legislación y procedimientos que prevean una respuesta oportuna y eficaz a las solicitudes, para maximizar, en la medida de lo posible, la probabilidad de que dicha asistencia tenga éxito.

Cooperación oficiosa

296. Dadas la importancia y urgencia potenciales de localizar y obtener datos relacionados con Internet en las investigaciones de actos de terrorismo, y la probabilidad de que esos datos estén en otro país, los investigadores necesitan considerar tanto los medios oficiales como los oficiosos. Si bien los canales oficiales de asistencia judicial recíproca pueden ofrecer mayor certidumbre en cuanto a las cuestiones jurídicas conexas, son más lentos y burocráticos que los canales oficiosos.

297. En la reunión del grupo de expertos, el experto del Canadá hizo hincapié en el papel crítico que había desempeñado la estrecha cooperación oficiosa entre la Real Policía Montada Canadiense y el Organismo Federal de Austria para la Protección del Estado y la Lucha contra el Terrorismo (Bundesamt für Verfassungsschutz und Terrorismusbekämpfung), facilitada por el funcionario de enlace del Canadá con base en

Viena, en cuanto al logro de un resultado positivo del enjuiciamiento. Además de ese caso, otros expertos mencionaron otros ejemplos similares en que la intervención de oficiales de enlace para facilitar la cooperación oficiosa había desempeñado un papel decisivo en la obtención de resultados satisfactorios.

298. Es probable que los datos relacionados con Internet, como los datos de uso de los abonados que tienen en su poder los proveedores de servicios de Internet, sean las pruebas decisivas en las causas de terrorismo en que se hayan usado computadoras e Internet. Si los investigadores pueden obtener la posesión física de las computadoras utilizadas por un sospechoso, así como los datos de uso conexos en poder de los proveedores de servicios de Internet, será más probable que puedan establecer el vínculo entre el sospechoso y el delito.

299. Teniendo esto presente, es importante que los investigadores y fiscales tengan plena conciencia de la posible importancia de los datos relacionados con Internet y la necesidad de adoptar medidas inmediatas para preservarlos de manera tal que garantice su admisibilidad como pruebas en cualquier procedimiento posterior. En la medida de lo posible, las fuerzas nacionales del orden deberían establecer, ya sea directamente con los proveedores de servicios de Internet o con los organismos homólogos de otros países, procedimientos claros, con la participación de medios tanto oficiales como oficiosos, encaminados a garantizar la retención y la entrega, con la mayor celeridad posible, de los datos de uso de Internet necesarios para la investigación penal.

300. En los Estados Unidos, donde tienen su sede muchos proveedores de servicios de Internet importantes, las autoridades siguen un criterio “dual” para ayudar a sus homólogos extranjeros en la retención y entrega de datos relacionados con Internet en poder de estos proveedores que operan en el país, para posibles fines probatorios. Con arreglo a este enfoque, las solicitudes extranjeras de retención y entrega de la información sobre las cuentas de los usuarios en poder de los proveedores de servicios de Internet podrían ser tramitadas de dos maneras:

- a) *Trámite oficioso.* Hay dos formas en que las autoridades investigadoras pueden conseguir por medios oficiosos la retención de los datos de Internet situados en los Estados Unidos: i) las autoridades extranjeras pueden establecer una relación directa con los proveedores de servicios de Internet y hacerles una petición oficiosa directa de que conserven y entreguen los datos solicitados; o ii) si no tienen ninguna relación directa, pueden hacer una petición oficiosa por conducto de la Oficina Federal de Investigaciones, que formula la solicitud a los proveedores de servicios;
- b) *Trámite oficial.* En este caso, las autoridades extranjeras pueden presentar una solicitud oficial de asistencia judicial recíproca para la entrega de los datos relacionados con la cuenta de un usuario en particular, por conducto de la Oficina de Asuntos Internacionales del Departamento de Justicia de los Estados Unidos. Una vez recibida la solicitud, la Sección de Lucha contra el Terrorismo del Departamento la examina para determinar si guarda relación con alguna investigación dirigida por los Estados Unidos. En caso negativo,

se envía la solicitud a un tribunal federal para que dicte la orden necesaria que autorice la obtención y transmisión de la información solicitada a las autoridades del país requirente.

301. Este último método de obtención de datos relacionados con los proveedores de servicios de Internet lo han utilizado con éxito las autoridades del Reino Unido y de los Estados Unidos en varias investigaciones de casos de terrorismo. En uno en particular, estos procedimientos dieron por resultado que un proveedor de servicios de Internet de los Estados Unidos proporcionara una cantidad considerable de datos de caché de Internet que fueron pruebas decisivas en un juicio en el Reino Unido.

F. Dificultades y problemas

302. Por su propia naturaleza, su huella geográfica virtual, su estructura fragmentaria y su rápida evolución, la tecnología de Internet presenta retos y problemas constantes a las fuerzas del orden y las autoridades de la justicia penal encargadas de la investigación y el enjuiciamiento de casos de terrorismo. En el debate de la reunión del grupo de expertos se destacaron algunas esferas que en ese momento eran problemáticas en relación con la cooperación internacional. En algunos casos, las dificultades para ejecutar las solicitudes de asistencia judicial recíproca y de extradición estaban relacionadas con el requisito de la doble incriminación. Varios expertos habían visto casos en que las solicitudes de asistencia judicial recíproca o de extradición se habían demorado o habían sido rechazadas por no satisfacer el requisito de la doble incriminación. En algunos casos, el problema residía en la incompatibilidad de las disposiciones penales, pero en otros había sido resultado de una interpretación excesivamente estricta de las disposiciones penales correspondientes por el poder judicial. Varios expertos consideraron que esta situación ponía de manifiesto la necesidad de impartir formación a los miembros de la judicatura en cuestiones de cooperación internacional.

1. Protección de la información confidencial

303. Los expertos de varios países se refirieron, en la reunión del grupo de expertos, a los problemas que seguían presentándose en relación con el intercambio de datos confidenciales de inteligencia entre, por un lado, las fuerzas del orden y los organismos de inteligencia nacionales y, por el otro, sus homólogos extranjeros. En los casos de terrorismo, las investigaciones y los juicios penales se basan, invariablemente, en la inteligencia reunida, por lo menos en las primeras etapas, lo que incluye información confidencial, protegida y de carácter reservado. La divulgación de esa información suele entrañar riesgos considerables, no solo para el organismo de donde proviene dicha información, sino también para el organismo o los organismos que la poseen, sobre todo cuando su divulgación podría comprometer, o llegar a comprometer, una investigación u operación en curso o futura.

304. La decisión de las autoridades nacionales de compartir o no esa información y, en caso afirmativo, en qué circunstancias, es una tarea compleja que requiere que se tomen en cuenta una serie de factores. Sin embargo, independientemente de los criterios

seguidos para evaluar el posible intercambio de información, en todos los casos y cualesquiera que sean las circunstancias, el organismo que comparta la información querrá asegurarse de que el organismo que la recibe mantenga las salvaguardias y garantías acordadas una vez que la tenga en su poder.

2. Soberanía

305. El concepto de soberanía, incluido el derecho de las naciones a determinar su propia condición política y ejercer soberanía permanente dentro de los límites de su jurisdicción territorial, es un principio ampliamente reconocido en las relaciones entre Estados y en el derecho internacional. Los casos que exigen investigaciones o enjuiciamientos de actividades transfronterizas de terroristas o de otros delincuentes pueden plantear problemas de soberanía a los países en que hay que realizar las investigaciones.

306. En algunos casos, las preocupaciones, válidas o no, que pueden tener las autoridades nacionales por percibir la investigación en su territorio como una injerencia en su soberanía nacional, pueden dificultar una cooperación internacional eficaz en investigaciones penales. Es importante, por tanto, que al examinar las medidas de investigación que requieren la obtención de pruebas relacionadas con computadoras o Internet, los investigadores y fiscales tengan presentes las consecuencias que esas diligencias de investigación podrían tener para la soberanía de otros Estados (por ejemplo, el registro a distancia, por las autoridades de un país, de una computadora usada por un sospechoso radicado en otro país).

307. En términos generales, en la medida de lo posible, las autoridades nacionales que estén considerando tomar medidas de investigación relativas a personas u objetos situados en otras jurisdicciones deberán notificar a sus homólogos de los países pertinentes y coordinar con ellos sus actividades.

3. Retención y entrega de información relacionada con Internet

308. Como se ha dicho, en muchos de los casos de terrorismo, una parte importante de las pruebas en contra de los presuntos autores está vinculada en algunos aspectos con actividades del sospechoso desarrolladas por Internet (por ejemplo, información sobre cuentas de tarjetas de crédito, información sobre el uso por los abonados de comunicaciones basadas en Internet, como el correo electrónico, VoIP, Skype, o relacionadas con redes sociales u otros sitios web). En muchos casos, será necesario que las autoridades investigadoras se aseguren de que se retengan y conserven los datos pertinentes de Internet para poder presentarlos con fines probatorios en actuaciones futuras. En este sentido, es importante señalar la distinción entre la “retención” y la “conservación” de los datos. En muchos países, los proveedores de servicios de Internet están obligados por ley a retener ciertos tipos de datos por un plazo determinado. La conservación, en cambio, se refiere a una obligación impuesta a un proveedor de servicios de Internet, en virtud de una resolución, orden o instrucciones judiciales de conservar los datos en condiciones determinadas para ser presentados como prueba en procesos penales.

309. Uno de los principales problemas que enfrentan todos los organismos encargados de hacer cumplir la ley es la falta de un marco convenido internacionalmente para la retención de los datos en poder de los proveedores de servicios de Internet. Mientras que los gobiernos de muchos países han impuesto obligaciones jurídicas a los proveedores de servicios de Internet locales de retener datos relacionados con Internet para la aplicación de la ley, a nivel internacional no existe ningún plazo estándar, acordado universalmente, durante el cual los proveedores estén obligados a retener esta información.

310. Por consiguiente, mientras que los investigadores de países que han impuesto la obligación de retener los datos a los proveedores de servicios de Internet tienen cierta seguridad, cuando realizan investigaciones exclusivamente dentro de su territorio, en cuanto al tipo de información de Internet que retendrán estos proveedores y durante cuánto tiempo, no puede decirse lo mismo de las investigaciones en que haya que obtener información que se encuentre en poder de un proveedor de otro país.

311. En los Estados Unidos, el método actual requiere que los proveedores de servicios de Internet conserven la información sobre el uso siempre que haya un pedido específico de un organismo encargado de hacer cumplir la ley, mientras que los proveedores siguen prácticas muy diversas en cuanto al plazo de retención, que puede ser de días o meses.

312. Si bien se han tomado algunas medidas para lograr cierta uniformidad en esta esfera, principalmente en la Unión Europea, ello ha sido problemático incluso a ese nivel. Con arreglo a la Directiva 2006/24/CE del Parlamento Europeo y del Consejo de la Unión Europea, de 15 de marzo de 2006, sobre la retención 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 modificaba la Directiva 2002/58/CE, en lo que se refiere a la retención de datos por los proveedores de servicios de comunicaciones electrónicas y las redes de comunicaciones públicas, los Estados miembros de la Unión Europea están obligados a garantizar que los proveedores regulados retengan los datos de comunicaciones específicas durante un período que varía entre seis meses y dos años. Sin embargo, a pesar de esta Directiva, no hay ningún período de retención de datos uniforme para todos los proveedores de servicios de Internet hospedados en la Unión Europea, y los períodos varían de seis meses a dos años como se estableció en la Directiva. En consecuencia, aunque hay mayor certeza sobre estos temas, incluso en el contexto de la Unión Europea existen diferencias en cuanto al tiempo durante el cual retienen los datos los proveedores de servicios de Internet que operan allí.

313. Varios participantes en la reunión del grupo de expertos opinaron que el desarrollo de un marco regulatorio universalmente aceptado que impusiera obligaciones uniformes a todos los proveedores de servicios de Internet en cuanto al tipo y período de retención de los datos de uso de los abonados sería de gran utilidad para los servicios de inteligencia y los organismos encargados de hacer cumplir la ley cuando investigan casos de terrorismo.

314. Como no existen normas ni obligaciones convenidas universalmente para los proveedores de servicios de Internet y otros proveedores de comunicaciones en relación con la retención de datos de Internet, es importante que en las investigaciones penales los investigadores y fiscales determinen cuanto antes si existen esos datos y el plazo pertinente; si es probable que sean de interés en un proceso; dónde se encuentran; y cuál es el plazo aplicable, si lo hubiere, durante el cual deba retenerlos el proveedor que los tenga en su poder. En caso de duda, sería prudente que las autoridades se pusieran en contacto con sus homólogos del país en que se encuentran los datos y tomaran las medidas (tanto oficiales como oficiosas) necesarias para garantizar la conservación de los datos para su posible entrega. Las autoridades, según las circunstancias del caso, incluidas su familiaridad o su relación con los proveedores de servicios de Internet, deberían considerar la posibilidad de ponerse en contacto directo con los proveedores y pedirles asistencia de manera oficiosa. Sin embargo, debido a la delicada situación en cuanto al cumplimiento de las leyes sobre la confidencialidad de la información de los usuarios y las leyes nacionales de privacidad, el grado de receptividad de los proveedores de servicios de Internet a las solicitudes oficiosas y directas puede variar considerablemente. En todo caso, siempre será prudente que los investigadores y fiscales se comuniquen y coordinen sus acciones con los homólogos extranjeros para garantizar la conservación y entrega de dicha información.

4. *Requisitos probatorios*

315. Para que las declaraciones, documentos y otra información puedan ser admitidos como pruebas en un proceso penal, los investigadores y fiscales necesitan tener sumo cuidado en cuanto a los métodos que utilicen para su reunión, conservación, presentación o transmisión y asegurarse de que estén en plena conformidad con las leyes, normas y principios jurídicos aplicables que rigen la práctica de las pruebas. Cualquier incumplimiento de los requisitos relativos a la admisibilidad de las pruebas puede menoscabar las alegaciones de la fiscalía, hasta el punto de que las autoridades puedan verse obligadas a sobreeser o retirar las acusaciones. En la causa *Namouh*, los fiscales canadienses pudieron conseguir, gracias a la estrecha colaboración con sus homólogos austríacos, que las pruebas vitales sobre el uso de salas de charla de Internet y sitios web por los acusados se reunieran y transmitieran al Canadá de manera tal que fueran admisibles, a pesar de las diferencias entre los dos países en cuanto a las normas probatorias.

316. En los casos de terrorismo, hay una serie de cuestiones que pueden plantear dificultades considerables a las autoridades en cuanto a la admisibilidad de determinados tipos de información. Sigue siendo un desafío para todos los funcionarios que participan en la investigación y persecución de casos relacionados con el terrorismo el superar las dificultades relativas a la admisibilidad de la información, ya que a menudo tienen características que la hacen inadmisibles. El carácter transnacional de los casos de terrorismo, incluido el uso generalizado de inteligencia (proporcionada a menudo por los asociados extranjeros con condiciones estrictas) o de métodos de registro, vigilancia e interceptación altamente especializados, muchas veces encubiertos e intrusivos, como base para la reunión de pruebas, puede presentar obstáculos importantes a las autoridades que quieran presentarlas como pruebas admisibles en un tribunal.

317. En el contexto del terrorismo, en lo que respecta específicamente a las dificultades probatorias que pueden surgir en relación con Internet o la tecnología informática, el planteamiento general adoptado por investigadores y fiscales sigue siendo el mismo. Entre las cuestiones de especial importancia estará, probablemente, la necesidad de conseguir, lo antes posible, la posesión física de computadoras o dispositivos similares supuestamente utilizados por los sospechosos; y la necesidad de adoptar medidas apropiadas, de acuerdo con las buenas prácticas reconocidas, para proteger la integridad de estos elementos de prueba (es decir, la cadena de custodia/de la prueba) y llevar a cabo un análisis forense digital si procede. Un incumplimiento de estos procedimientos podría afectar la admisibilidad de este tipo de pruebas. Entre otras formas de pruebas que pueden exigir especial atención cabe mencionar el material obtenido como resultado de las actividades de registro o vigilancia, o ambas, que deben llevarse a cabo únicamente con la debida autorización judicial.

318. Cuando se tratan cuestiones probatorias en la etapa de la investigación, es importante que los investigadores tengan una idea clara de las normas y de los principios jurídicos aplicables a las indagaciones realizadas como parte de una investigación, y que se mantengan en comunicación estrecha con los fiscales, manteniéndolos informados y pidiéndoles asesoramiento jurídico. En los casos en que las autoridades reúnen pruebas en un país para usarlas en un juicio en otro país, es muy importante que exista comunicación y coordinación estrechas con los homólogos extranjeros sobre las medidas que se están adoptando para reunir las pruebas y conservarlas. Como parte de esa coordinación, es importante que las autoridades encargadas de las investigaciones entiendan claramente los requisitos probatorios y las consecuencias que acarrearán sus actos en la jurisdicción donde, en definitiva, se utilizarán las pruebas. Las cuestiones relacionadas con la admisibilidad de pruebas obtenidas en el extranjero en los casos relacionados con el terrorismo se tratan de manera más amplia en el *Compendio de casos relativos a la lucha contra el terrorismo* de la UNODC¹⁵³.

5. Doble incriminación

319. Un requisito que se encuentra comúnmente en los instrumentos universales contra el terrorismo y en otros instrumentos internacionales, regionales y bilaterales relacionados con el terrorismo y la delincuencia organizada transnacional es que solo la conducta ilícita que esté tipificada tanto en el Estado requirente como en el requerido puede constituir la base para la cooperación internacional. Este requisito, conocido como “doble incriminación”, puede presentar dificultades en todas las investigaciones y causas penales, no solo en las relacionadas con el terrorismo sino también en las que se necesite algún elemento de cooperación internacional. Varios participantes en la reunión del grupo de expertos opinaron que la cuestión de la doble incriminación era un problema fundamental, que llevaba con frecuencia al rechazo de las solicitudes de extradición o de asistencia judicial recíproca cuando las autoridades de los países requeridos consideraban que no se cumplía el requisito de la doble incriminación.

¹⁵³ Véase Oficina de las Naciones Unidas contra la Droga y el Delito, *Compendio de casos relativos a la lucha contra el terrorismo*, párrs. 292 a 295.

320. En el contexto del terrorismo, como no existe una obligación universal de que los Estados tipifiquen como delito cierta conducta ilícita específica realizada por Internet, las autoridades centrales suelen basarse, al hacer o recibir solicitudes de cooperación internacional, en los delitos establecidos en la legislación relacionada con el terrorismo o en sus códigos penales nacionales. Por ejemplo, en el caso de presuntos actos de incitación al terrorismo que se cometen por Internet, debido a las diferencias de los criterios jurídicos adoptados por los Estados con respecto a dicha conducta, puede resultar necesario basar las solicitudes de cooperación internacional en actos delictivos preparatorios tales como el de instigación.

321. Para abordar este problema, es conveniente que los gobiernos, cuando tipifican como delito la conducta ilícita requerida asociada con el terrorismo, creen figuras delictivas que sean lo más parecidas posible a las mencionadas en los instrumentos pertinentes. Además, en la medida en que lo permitan los ordenamientos jurídicos nacionales, la legislación debería redactarse de manera que no fuera indebidamente estricta con respecto a la cuestión de la doble incriminación, proporcionando así a las autoridades centrales y los jueces suficiente latitud para considerar y evaluar solo lo esencial de la conducta ilícita que sea objeto de la solicitud, en lugar de adoptar un enfoque indebidamente rígido. Si los Estados adoptaran este enfoque legislativo de manera uniforme, se lograría todo el beneficio de la armonización legislativa perseguida por los instrumentos y se reducirían los problemas potenciales de la doble incriminación.

322. Si bien las cuestiones relativas a la doble incriminación pueden crear dificultades en causas penales en las que se necesita la cooperación internacional en general, pueden ser especialmente problemáticas en los casos relacionados con ciertos delitos de terrorismo cometidos por Internet (por ejemplo, la incitación) en que el riesgo de incompatibilidad entre los marcos legislativos y constitucionales nacionales de los Estados correspondientes es aún mayor. Un ejemplo, examinado en la reunión del grupo de expertos, se refiere a la posición de los Estados Unidos en relación con la extradición de personas acusadas del delito de incitación. En ese país, hay fuertes garantías constitucionales de la libertad de expresión, consagradas en la Primera Enmienda de la Constitución de los Estados Unidos. En virtud de la legislación de los Estados Unidos, las declaraciones equivalentes a una apología independiente de cualquier posición política, religiosa o ideológica no se consideran actos delictivos *per se*, pese a que podrían constituir actos equivalentes al suministro de información siguiendo las instrucciones de una organización terrorista o a fin de controlarla, o estar comprendidos en el ámbito del delito de instigación. Habida cuenta de esta posición, las solicitudes de extradición o de asistencia judicial recíproca por presuntos actos de incitación en que algún elemento del delito tenga lugar dentro de los Estados Unidos podrían resultar problemáticas por la doble incriminación, obligando a las autoridades de ambos países a adoptar un enfoque flexible y pragmático.

323. Además de tener legislación compatible y un enfoque flexible para la aplicación de esas leyes, es importante que los investigadores, los fiscales y la judicatura tengan una formación sólida y entiendan cómo funcionan los mecanismos de cooperación internacional en la respuesta de la comunidad internacional al terrorismo y a la delincuencia organizada transnacional.

6. *Diferencias en la aplicación de las garantías constitucionales y de los derechos humanos*

324. Las cuestiones relativas a los derechos humanos y las garantías constitucionales están vinculadas con muchos aspectos de la investigación y el enjuiciamiento del terrorismo, incluidos los de la cooperación internacional. Para usar una vez más los actos relativos a la incitación al terrorismo como ejemplo, se comprueba que los diferentes enfoques nacionales de la aplicación de los derechos constitucionales y los derechos humanos reflejan criterios jurídicos diversos. Esto puede crear dificultades en los casos de cooperación internacional en que los Estados tratan de solicitar o proporcionar asistencia. Por ejemplo, cuando las autoridades de un país presentan una solicitud a sus homólogos de otro país requiriendo datos relacionados con Internet relativos a declaraciones hechas por Internet que configuran la incitación a cometer actos de terrorismo en su jurisdicción, será importante determinar si los supuestos actos también están tipificados como delito en el Estado requerido. En el contexto más amplio del control del contenido de Internet, cuando las autoridades de un país quieren que se retire el contenido que consideran incitación al terrorismo, y que está hospedado en un servidor que se encuentra en otra jurisdicción, hay que tener en cuenta que pueden diferir las leyes aplicables y las garantías constitucionales de derechos, como el derecho a la libertad de expresión.

325. La situación de algunos tipos de correo electrónico relacionados con el terrorismo o contenidos de Internet que han sido encaminados a través de proveedores de servicios de Internet con sede en los Estados Unidos, o almacenados por ellos, reviste especial importancia. Según el carácter y contexto de los contenidos, esos casos, que son de competencia de los Estados Unidos, pueden ser problemáticos debido a la gran protección con que cuenta la libertad de expresión en la Primera Enmienda de la Constitución de ese país. En estos casos, las autoridades de diferentes países necesitan mantener una comunicación estrecha para determinar qué medidas preventivas o de procesamiento pueden tomarse, si corresponde, que sean compatibles con sus respectivas legislaciones, sus normas jurídicas y culturales y sus obligaciones internacionales de lucha contra el terrorismo.

7. *Competencia concurrente*

326. Los casos de terrorismo en que los elementos del delito se llevan a cabo por Internet pueden plantear complejas cuestiones de competencia, especialmente cuando un presunto delincuente se encuentra en un país y utiliza para cometer el delito sitios de Internet o servicios de proveedores de servicios de Internet hospedados en otro. Ha habido casos en que personas residentes en un país han creado, administrado y mantenido sitios Web en otro país, para promover la yihad y con otros fines relacionados con el terrorismo.

327. El caso belga de *Malaki el Aroud y otros* (véase el párrafo 377) es un buen ejemplo de ello. La acusada, que vivía en Bélgica, administraba un sitio web, hospedado en el Canadá, que usaba para la promoción de la yihad y con otros fines de apoyo a actividades terroristas. El procesamiento de actividades relacionadas con el

terrorismo en estas situaciones depende en gran medida de una cooperación internacional eficaz.

328. No hay reglas vinculantes en el derecho internacional que traten el tema de cómo deben los Estados dirimir los conflictos de competencia cuando más de un Estado puede pretender conocer de un delito imputable al mismo sospechoso. A pesar de que los Estados tienen amplias facultades discrecionales con respecto a los criterios aplicables, esto implica sopesar o evaluar diferentes factores. Estos pueden incluir la “conectividad” entre el presunto delito y ciertos Estados, incluidos la nacionalidad del sospechoso, el lugar de la comisión de los actos que configuran el delito, dónde se encuentran los testigos y las pruebas del caso, y las posibles dificultades para reunir, transmitir o producir las pruebas en una jurisdicción en particular. En algunos Estados, incluidos Bélgica, el Canadá y España, se considera que ciertas formas de competencia son subsidiarias de las demás. Se considera que los Estados que tienen conexiones estrechas con un delito (por ejemplo, el delito se cometió en su territorio o fue cometido por uno de sus nacionales) tienen competencia primaria, mientras que los Estados que tengan competencia en virtud de otras razones, la ejercerán únicamente cuando el Estado con competencia primaria no quiera o pueda hacer ejercicio de la acción penal¹⁵⁴.

329. Algunos países, incluido el Canadá, siguen un criterio de “conexión real y esencial” para determinar si tienen competencia en materia penal¹⁵⁵. En Israel, cuando se reciben solicitudes de cooperación internacional de otros países, se realizan investigaciones dentro del país para determinar si puede probarse que, según el derecho israelí, se cometió un delito que debería ser enjuiciado allí. Si la investigación no da por resultado la iniciación de una acción penal, las autoridades israelíes remiten todas las pruebas disponibles [y trasladan al presunto delincuente] a través de los canales oficiales al país requirente para que allí se realice el procesamiento. En el Reino Unido, la legislación y la jurisprudencia sobre ciertos delitos relacionados con el terrorismo cuya comisión supone la realización de actividades fuera de su territorio (incluso por medio de Internet) permiten que las autoridades británicas ejerzan su competencia si se puede demostrar que una “medida considerable” de las actividades constitutivas del delito ocurrieron en su país, y si se puede argumentar razonablemente que esas actividades no deben ser tratadas en otro país.

330. Al resolver problemas relativos a la competencia concurrente o a la cooperación internacional, las autoridades centrales (fiscales, las más de las veces) deben tener conciencia, desde un comienzo, de que existe una necesidad de comunicarse y colaborar cuanto antes con sus homólogos de otras jurisdicciones que puedan tener interés en iniciar un proceso contra el mismo presunto delincuente. La decisión de cuándo y cómo iniciar esta comunicación debe tomarse caso por caso, después de un examen exhaustivo de los distintos factores que podrían estar en juego en cada caso particular. Los fiscales que están considerando dichas cuestiones pueden encontrar orientación útil en

¹⁵⁴Asociación Internacional de Abogados, División de Práctica Forense, *Report of the Task Force on Extraterritorial Jurisdiction* (2008), págs. 172 y 173.

¹⁵⁵*R. c. Hape* [2007] 2 SCR. 292, 2007 SCC 26, párr. 62.

“Guidance for Handling Criminal Cases with Concurrent Jurisdiction between the United Kingdom and the United States” [Orientación para la tramitación de causas penales en casos de competencia concurrente entre los Estados Unidos y el Reino Unido], de 2007, publicada por las Fiscalías Generales de los Estados Unidos y el Reino Unido¹⁵⁶, que prevé en el contexto “de las causas penales más graves y delicadas o complejas” (a las que se refiere el informe) mejores métodos de intercambio de información y comunicación entre las fiscalías de los dos países. Para ayudar a determinar si hay que iniciar ese contacto, el informe sugiere que el fiscal de un país se formule la siguiente pregunta: “¿existe alguna posibilidad real de que un fiscal [del otro país] pueda tener interés en enjuiciar? Los casos de este tipo suelen tener conexiones importantes [con el otro país]”. Mientras que el momento y el método seguido para establecer la comunicación sobre temas de cooperación internacional y jurisdiccional variarán según las circunstancias de cada caso particular, los fiscales deberían considerar la formulación de esa pregunta como una guía útil para orientar su labor.

8. *Leyes nacionales de protección de datos y de la privacidad*

331. La legislación nacional sobre la protección de los datos personales o de la privacidad suele restringir la capacidad de los organismos encargados de hacer cumplir la ley y de inteligencia para intercambiar información con sus homólogos nacionales y extranjeros. Una vez más, encontrar el equilibrio justo entre el derecho humano a la privacidad y los intereses legítimos del Estado de investigar y enjuiciar eficazmente un delito es un desafío constante para los gobiernos y, en algunos casos (incluidas las respuestas al terrorismo), ha suscitado inquietudes¹⁵⁷.

332. Además de contar con legislación que proporcione orientación clara a los investigadores, fiscales y, en el caso de los datos de Internet, a los proveedores de servicios de Internet que tengan datos en su poder, sobre las obligaciones relativas a la reunión y utilización de datos personales, es igualmente importante que los países establezcan y pongan en funcionamiento mecanismos eficaces para supervisar a los organismos encargados de hacer cumplir la ley y los de inteligencia. Los gobiernos deben asegurarse de que sus legislaciones nacionales incluyan los mecanismos apropiados para que las autoridades puedan compartir, con sujeción a las garantías del derecho a la privacidad que correspondan, la información pertinente para la investigación y el enjuiciamiento de casos de terrorismo con sus homólogos nacionales y extranjeros.

9. *Las solicitudes basadas en tratados frente a las carentes de ese fundamento*

333. Las respuestas nacionales a las solicitudes de cooperación que no se basan en ningún tratado difieren, ya que algunos países están limitados en cuanto a prestar cooperación oficial en ausencia de un tratado. En reconocimiento de esta situación, los

¹⁵⁶Se puede consultar en www.publications.parliament.uk/pa/ld200607/ldlwa/70125ws1.pdf.

¹⁵⁷Véase el informe del Relator Especial correspondiente a 2009 sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo (A/HRC/10/3), en que este expresó preocupación por la incursión en los derechos individuales a la privacidad causada por la intensificación de la vigilancia y del intercambio de inteligencia entre los organismos del Estado.

instrumentos universales contra el terrorismo y la delincuencia organizada transnacional prevén que ellos mismos puedan ser usados como fundamento jurídico para la cooperación y para que ciertas conductas ilícitas determinadas sean tratadas como delito, a los fines de la asistencia judicial recíproca y la extradición, por las leyes nacionales de los Estados partes.

334. Muchos países, entre ellos China, se guían por el principio de reciprocidad como base para la cooperación internacional. Según la legislación china, los organismos encargados de hacer cumplir la ley y las autoridades judiciales pueden prestar cooperación internacional, incluida la asistencia mutua o asistencia judicial recíproca (incluida la extradición), en el marco de un tratado. En ausencia de este, la reciprocidad también puede ser un fundamento jurídico para la asistencia judicial recíproca y la cooperación para la extradición. En la reunión del grupo de expertos, el experto de China mencionó un ejemplo de cooperación eficaz entre las autoridades de China y las de los Estados Unidos que llevó al cierre del sitio web de pornografía más grande del mundo, en chino, que se hospedaba en los Estados Unidos y estaba destinado a usuarios de Internet de China y otros países asiáticos.

335. Varios participantes en la reunión del grupo de expertos se refirieron a las cuestiones relativas al carácter confidencial de gran parte de la información (a menudo basada en inteligencia) relacionada con las investigaciones del terrorismo y las dificultades inherentes, no solo en el contexto de la cooperación internacional sino también a nivel nacional, que enfrentan los organismos que desean compartir esa información con sus homólogos. Varios expertos subrayaron que la información era a menudo de carácter sumamente delicado y que el intercambio resultaba difícil en ausencia de un mecanismo de intercambio de información oficial que impusiera las condiciones apropiadas en cuanto a su uso y divulgación.

336. Este tema se examina con mayor profundidad en el siguiente capítulo, sobre los procesos judiciales, en el contexto de las cuestiones probatorias relacionadas con la admisibilidad de datos de inteligencia como prueba y la revelación de pruebas en los procesos penales.

VI. El proceso penal

A. Introducción

337. Parte integrante del marco jurídico universal contra el terrorismo, y de la Estrategia global de la Naciones Unidas contra el terrorismo, es la obligación impuesta a los Estados de denegar refugio y llevar ante la justicia a los responsables de actos terroristas, dondequiera que se cometan. A fin de lograr el último de estos objetivos, los países necesitan contar no solo con una legislación eficaz contra el terrorismo, que tipifique los actos terroristas y facilite la cooperación internacional necesaria, sino también con la capacidad para aplicar estrategias de enjuiciamiento y técnicas de investigación especializadas que garanticen la reunión, conservación, entrega y admisibilidad de las pruebas (basadas muchas veces en inteligencia) cuando se enjuicie a presuntos terroristas, y que, al mismo tiempo, garanticen la observancia de las normas internacionales de trato de los acusados.

338. La función de los fiscales en el enjuiciamiento de casos de terrorismo se ha vuelto cada vez más compleja y difícil. Además de estar encargados de entablar las acciones penales que procedan, los fiscales tienen cada vez mayor participación en las fases de investigación y reunión de inteligencia en los casos de terrorismo, proporcionando orientación o supervisión sobre las consecuencias jurídicas y estratégicas de las diversas técnicas de investigación. En el presente capítulo, se examina la función de los fiscales en los casos de uso de Internet por terroristas, con miras a determinar, desde la perspectiva del fiscal, cuáles son los obstáculos o dificultades frecuentes que deben superarse, y qué estrategias y enfoques llevan al éxito del enjuiciamiento de los responsables.

B. Enfoque del proceso penal basado en el estado de derecho

339. Si la investigación y el procesamiento no se llevan a cabo de plena conformidad con los principios asociados generalmente con el estado de derecho y las normas internacionales de derechos humanos, se comprometerá la integridad de la estructura misma de las normas sociales e institucionales que los propios terroristas procuran socavar. Es de importancia fundamental, por tanto, que todo enjuiciamiento de los autores de actos de terrorismo se realice prestando especial atención a la necesidad de garantizar un juicio imparcial y un trato justo de los acusados.

340. El principio, ampliamente reconocido, de que los presuntos sospechosos de terrorismo deben gozar de las mismas garantías procesales en el marco del derecho penal que cualquier otro presunto delincuente está profundamente arraigado y encuentra

expresión en los instrumentos universales de lucha contra el terrorismo y, a nivel político, en el plano internacional. Entre los muchos ejemplos del alto nivel de reconocimiento de este principio, cabe mencionar la resolución 59/195 de la Asamblea General, relativa a los derechos humanos y el terrorismo, en que la Asamblea destacó la necesidad de mejorar las medidas de cooperación internacional de lucha contra el terrorismo, de conformidad con el derecho internacional, incluidas las normas internacionales de derechos humanos y el derecho humanitario. Además de incorporar este principio fundamental en el plano político, las Naciones Unidas, por conducto de su Relator Especial sobre la promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, informa periódicamente al Consejo de Derechos Humanos y a la Asamblea General sobre los temas motivo de preocupación relacionados con los aspectos de los derechos humanos afectados por las medidas de la justicia penal contra el terrorismo y hace recomendaciones para que las instancias correspondientes adopten medidas correctivas. Las cuestiones planteadas por el Relator Especial incluyen las relacionadas con la detención y la acusación de sospechosos¹⁵⁸.

341. Hay varias publicaciones que examinan específicamente y tienden a promover el respeto de los derechos humanos y el estado de derecho dentro de las atribuciones de los fiscales y funcionarios de la justicia penal en los juicios de terrorismo. En 2003 la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos preparó el *Resumen de jurisprudencia de las Naciones Unidas y las organizaciones regionales sobre la protección de los derechos humanos en la lucha contra el terrorismo*. En el Consejo de Europa, que ha reconocido e integrado plenamente la obligación de aplicar salvaguardias para los derechos humanos como principio fundamental en sus instrumentos relacionados con la prevención del delito y los problemas de la justicia penal, incluido el terrorismo, este principio se reafirma en las Directrices del Comité de Ministros del Consejo de Europa sobre los derechos humanos y la lucha contra el terrorismo, aprobadas por el Comité de Ministros el 11 de julio de 2002¹⁵⁹. Estos documentos proporcionan una orientación valiosa a los fiscales que trabajan en el campo de la lucha contra el terrorismo.

C. Función del fiscal en los casos de terrorismo

342. El papel del fiscal en los procedimientos penales, incluidos los casos de terrorismo, varía de un país a otro. En algunos países, particularmente en jurisdicciones de tradición romanista, los fiscales están oficialmente encargados de seguir de cerca la marcha de las investigaciones penales, supervisar los equipos de investigadores en el curso de la investigación, tomar decisiones sobre las actividades de registro y vigilancia, presentar cargos o acusaciones, encargarse de las cuestiones de cooperación internacional y ocuparse de las actuaciones ante los tribunales.

¹⁵⁸Ibid.

¹⁵⁹Todo texto creado en el seno del Consejo de Europa, independientemente de que se trate de un convenio vinculante o de un instrumento de "derecho incipiente", como una recomendación o resolución aprobada por la Asamblea Parlamentaria o el Comité de Ministros, incluidas las directrices sobre diversos temas, debe estar siempre en consonancia con la copiosa jurisprudencia del Tribunal Europeo de Derechos Humanos sobre el tema de que se trate.

343. En un sistema judicial inquisitivo como el francés, por ejemplo, el fiscal está generalmente encargado de iniciar la acción penal y las investigaciones preliminares, así como de encuadrar los hechos en las figuras delictivas; sin embargo, un juez de instrucción dirige la investigación judicial oficial, reuniendo y examinando las pruebas. Cuando puede excluirse la culpabilidad del sospechoso, el juez de instrucción cierra las actuaciones; de lo contrario, el procesado es puesto a disposición de otro juez para su enjuiciamiento. En casos de terrorismo, además de presentar pruebas de cargo a un juez, el fiscal principal puede solicitar o presentar una petición para que se realicen más investigaciones.

344. En otros países, en particular en las jurisdicciones que tienen el sistema del *common law*, los fiscales han tenido tradicionalmente menor participación directa o responsabilidad en la realización de investigaciones penales, que normalmente están dirigidas por organismos encargados de hacer cumplir la ley. Normalmente, en estas jurisdicciones, los fiscales comienzan a tener la responsabilidad oficial de enjuiciar cuando presentan los cargos o la acusación hasta la terminación del proceso. Por ejemplo, en Nigeria, la policía nacional es responsable de llevar a cabo las investigaciones penales. Una vez concluidas, los casos se derivan al ministerio público, que tiene la responsabilidad de imputar delitos e intervenir en los procesos penales.

345. Se sigue un enfoque similar en Indonesia, donde existe una separación con respecto a la investigación y la prosecución de un caso penal. Después del inicio de una investigación penal, el investigador debe informar sobre la marcha de la investigación a la fiscalía (art. 109, párrafo 1, del Código de procedimiento penal de Indonesia) y, una vez concluida la investigación, debe pasar las actuaciones al ministerio público (art. 110, párrafo 1, del Código de procedimiento penal), que decide entonces si el caso puede ser llevado a juicio (art. 139 del Código de procedimiento penal).

346. Sin embargo, independientemente de las características específicas de la jurisdicción de que se trate, el papel desempeñado por los fiscales en los casos de terrorismo sigue evolucionando para satisfacer la mayor demanda creada por los cambios constantes en el tipo, los métodos y la complejidad de los delitos relacionados con el terrorismo, las leyes de lucha contra el terrorismo, las nuevas técnicas de investigación y los acuerdos de cooperación internacional.

347. La experiencia demuestra que los fiscales se ven cada vez más obligados a tener una participación más directa en la investigación de los delitos, y no solo durante la fase de actuación de la fiscalía. Los fiscales están adoptando con mayor frecuencia una función más estratégica y técnica, no solo fundamentando la política y legislación de lucha contra el terrorismo, sino también proporcionando, durante las investigaciones, orientación jurídica y estratégica sobre las cuestiones jurídicas que inciden en las probabilidades de éxito de cualquier enjuiciamiento que se realice. La experiencia enseña que tienden a asumir su función como parte de un equipo multidisciplinario o multijurisdiccional¹⁶⁰.

¹⁶⁰Yvon Dandurand, "The role of prosecutors in promoting and strengthening the rule of law", documento presentado en la Segunda Cumbre Mundial de Fiscales, Procuradores Generales y Jefes de Ministerios Públicos, celebrada en Doha, del 14 al 16 de noviembre de 2005.

348. Por otra parte, con una mayor visibilidad y exámenes más rigurosos de los juicios de terrorismo, incluida la cobertura de los medios de comunicación y la supervisión por parte de grupos de derechos humanos y organismos internacionales, los fiscales desempeñan un papel decisivo para garantizar que las investigaciones y actuaciones judiciales no solo sean imparciales y eficientes y se realicen con pleno respeto de las normas internacionales de los derechos humanos, sino que sean percibidas como tales.

D. Fase de la investigación

349. Durante la fase de reunión de inteligencia o investigativa de las operaciones de lucha contra el terrorismo, los fiscales suelen verse en la necesidad de prestar asesoramiento jurídico sobre cuestiones relacionadas con el uso de técnicas de investigación especializadas.

1. Técnicas de investigación especializadas

350. Si bien la tecnología y las técnicas de registro y vigilancia nuevas o emergentes proporcionan inteligencia y mayores oportunidades a los organismos encargados de hacer cumplir la ley de concentrar la atención en las actividades terroristas por Internet, también acarrearán riesgos jurídicos en el contexto de los enjuiciamientos, que los fiscales deben tener siempre en cuenta. Además, debido a las diferencias en las leyes nacionales relacionadas con la reunión y admisión de las pruebas, estos riesgos son mayores cuando los actos se cometen —y dejan pruebas— en una jurisdicción diferente de donde se llevará a cabo el proceso. A nivel europeo, el Consejo de Europa, consciente de esos riesgos y de las cuestiones de derechos humanos que implican, ha elaborado una recomendación sobre técnicas de investigación especiales en relación con los delitos graves, incluidos los actos de terrorismo¹⁶¹, que contiene, entre otras cosas, principios generales, directrices operacionales y un capítulo sobre cooperación internacional.

351. Los riesgos jurídicos relacionados con las nuevas técnicas de investigación refuerzan la necesidad de que los fiscales participen activamente, desde un principio, en la adopción de decisiones durante la fase de investigación de los casos de terrorismo para asegurarse de que las medidas adoptadas en la obtención de pruebas potenciales no pongan en peligro el éxito de cualquier proceso posterior. Las cuestiones relacionadas con la admisibilidad de las pruebas se tratan con más detalle más adelante en este mismo capítulo.

352. Los cambios constantes y rápidos en la capacidad tecnológica de los servicios de inteligencia y los organismos encargados de hacer cumplir la ley con respecto a la vigilancia, la monitorización y la reunión de inteligencia o de las pruebas de actividades terroristas ponen de relieve la importancia fundamental de la función del fiscal de prestar asesoramiento a los investigadores sobre las consecuencias jurídicas de sus actividades en el proceso. Además, debido a la creciente probabilidad, en particular en los

casos de actividades transfronterizas por Internet, de que las autoridades necesiten coordinar su labor y colaborar con sus homólogos extranjeros sobre cuestiones jurídicas conexas (por ejemplo, la conservación de los datos de Internet en poder de los proveedores de servicios de Internet), es cada vez más importante que se consulte a los fiscales y se les haga participar en las decisiones sobre las estrategias de investigación tan pronto como sea posible.

2. *El uso de equipos multidisciplinarios*

353. Las autoridades están recurriendo, cada vez más, a equipos multidisciplinarios o interinstitucionales, integrados por organismos policiales y de inteligencia, así como por fiscales, para la interdicción, el desbaratamiento y el enjuiciamiento de las actividades terroristas. El alto nivel de confianza, coordinación y comunicación que se consideró vital en la reunión del grupo de expertos para la cooperación eficaz a nivel internacional también debe existir, a nivel nacional, entre los organismos de aplicación de la ley, los servicios de inteligencia y las fiscalías. Aunque no existe ningún enfoque único que permita armonizar estos elementos, una comprensión clara de los mandatos y las funciones de los organismos participantes, la disponibilidad de facultades y mecanismos de intercambio de información apropiados (basados quizá en memorandos de entendimiento o acuerdos similares) y la organización de reuniones de coordinación periódicas o de actividades de capacitación servirían para fortalecer estas importantes asociaciones nacionales.

354. Si bien hay diferencias en la forma en que las autoridades de diferentes países llevan y coordinan las investigaciones en que interviene más de un organismo, hay sin embargo amplias similitudes. En los Estados Unidos, se emplea el enfoque del grupo de tareas, que usa equipos multidisciplinarios de todos los organismos pertinentes, incluidas las fiscalías, para realizar las investigaciones relacionadas con el terrorismo en ese país.

355. Con arreglo a ese criterio, los fiscales se incorporan e integran en los equipos de inteligencia, policiales y de otros organismos especializados, que constantemente monitorizan, evalúan y reevalúan diferentes aspectos de las investigaciones de una presunta actividad terrorista. Los grupos de tareas contra el terrorismo o los grupos de tareas conjuntos, o ambos, coordinan las actividades de los organismos encargados de hacer cumplir la ley y de las fiscalías locales, estatales y federales. Muchas fiscalías estatales y federales participan en estos grupos de tareas, siguiendo métodos y realizando actividades tan diferentes como asistir a reuniones interinstitucionales, compartir oficinas comunes, prestar asesoramiento jurídico para la obtención de órdenes de registro, o examinar los casos y formular recomendaciones sobre el encuadre jurídico¹⁶².

¹⁶²M. Elaine Nugent y otros, *Local Prosecutors' Response to Terrorism* (Alexandria, Virginia, American Prosecutors Research Institute, 2005).

356. En el Canadá, las autoridades utilizan equipos integrados de ejecución de la ley y de seguridad nacional (INSET). En el caso de Namouh, el equipo integrado estaba formado por miembros de la Real Policía Montada del Canadá, la Agencia de Servicios Fronterizos del Canadá, el Servicio de Inteligencia de Seguridad del Canadá, la Policía Provincial de Quebec, el Servicio de Policía de Montreal y el Ministerio Público del Canadá.

357. En el Japón, es práctica común que durante las investigaciones relacionadas con el terrorismo realizadas por la policía, esta informe al ministerio público, a pesar de ser instituciones jurídicamente independientes, en las primeras etapas de la investigación y consulte con los fiscales al evaluar las pruebas e interpretar las leyes¹⁶³. En Egipto se aplica un enfoque similar.

358. A fin de aumentar la eficacia y eficiencia de los procesos penales de terrorismo, los gobiernos suelen crear, dentro del ministerio público nacional, dependencias o departamentos especializados que se ocupan de los casos relacionados con el terrorismo. Este es el caso de Indonesia, que ha adoptado una serie de medidas especiales, incluida la creación de un equipo de tareas dentro de la Fiscalía General para el enjuiciamiento de actos de terrorismo y delitos transnacionales. Este equipo de tareas se encarga de facilitar y agilizar la aplicación de la ley, tanto durante la fase de investigación, mediante la coordinación con la policía (por ejemplo, haciendo participar a los fiscales del Estado en los interrogatorios de los sospechosos), como en la fase subsiguiente del enjuiciamiento, hasta terminar con la ejecución de la sentencia.

359. Aunque es posible que haya variaciones a nivel internacional en la manera en que los fiscales participan y se integran en las investigaciones penales, el enfoque general adoptado en muchos países destaca la conveniencia de dicha integración y de seguir un enfoque holístico e interdisciplinario cuando se toman decisiones estratégicas y operacionales durante la etapa de investigación de actos de terrorismo.

E. Cooperación internacional

360. Las cuestiones relacionadas con la cooperación internacional ya han sido tratadas en el capítulo VI *supra* y no es necesario reiterarlas aquí. Las cuestiones concretas de interés para los fiscales, planteadas por los participantes en la reunión del grupo de expertos, en los casos que presentan elementos de cooperación internacional se refieren a la mediación y resolución de cuestiones relacionadas con el modo de cooperación, los conflictos de competencia, el requisito de la doble incriminación y la admisibilidad de las pruebas obtenidas en el extranjero, que por experiencia se sabe que presentan un reto permanente. Habida cuenta del interés común de todos los Estados en el enjuiciamiento eficaz de los delitos relacionados con el terrorismo, es importante no solo que los Estados cuenten con el marco legislativo para facilitar esta cooperación,

¹⁶³ Oficina de Naciones Unidas contra la Droga y el Delito, *Compendio de casos relativos a la lucha contra el terrorismo*, párr. 212.

sino también que los fiscales se encarguen de la resolución de estas cuestiones de manera proactiva y recurriendo a la colaboración.

F. Fase acusatoria

1. *La decisión de acusar*

361. En la mayoría de los países, los fiscales tienen amplia discreción para decidir si han de iniciar la acción penal y determinar los cargos. A menudo esas decisiones se toman de conformidad con directrices o códigos que tienen por objeto asegurar el ejercicio de esta facultad de manera justa, transparente y consecuente. Por ejemplo, en el Reino Unido, los fiscales adoptan estas decisiones de acuerdo con el Código para los Fiscales de la Corona, que proporciona un umbral para acusar basado en la suficiencia de la prueba y el interés público. Los fiscales deben estar convencidos de que con las pruebas que tienen en su poder hay una “posibilidad realista de obtener una condena” antes de acusar a un sospechoso de la comisión de un delito determinado¹⁶⁴. En Egipto se sigue un enfoque similar.

362. En el contexto del terrorismo, el elemento del interés público es muy importante cuando se considera si se debe acusar, dada la necesidad, siempre que sea posible, de enjuiciar los actos terroristas o delitos conexos para proteger al público y prevenir la comisión de delitos similares. En muchos casos, las cuestiones relativas a la suficiencia de las pruebas disponibles pueden ser factores determinantes que pueden verse afectados por la posibilidad de utilizar pruebas basadas en inteligencia que no comprometan sus fuentes y métodos de reunión u otras investigaciones. Por esta razón, en algunos casos los fiscales pueden verse obligados a optar por acusar a los sospechosos de la comisión de delitos que no son de terrorismo propiamente dicho para proteger la integridad de los datos de inteligencia.

2. *Uso de figuras delictivas generales o no específicas de actos terroristas*

363. En los casos en que hay que intervenir para impedir la comisión de actos terroristas antes de que haya pruebas suficientes para iniciar un proceso por la preparación de esos actos, es posible que las autoridades necesiten encuadrar los actos en otras figuras delictivas para dar una base jurídica a sus acciones. En muchos casos en que presuntos terroristas han utilizado Internet como parte de las actividades delictivas, las autoridades han empleado con éxito los delitos de instigación, confabulación, participación en grupos terroristas o prestación de apoyo material a estos, en lugar de los delitos en sí que planeaban cometer. En este contexto, contar con figuras como la instigación, confabulación o asociación ilícita es particularmente útil. En algunos casos, las autoridades han recurrido a alguna otra figura penal general como el fraude o delitos relacionados con la tenencia o uso de artículos ilegales (por ejemplo, documentos de identidad o de viaje falsos, armas),

¹⁶⁴Ministerio Público de la Corona, “The Code for Crown Prosecutors” (Londres, 2010). Se puede consultar en www.cps.gov.uk/publications/docs/code2010english.pdf.

que permiten a los investigadores y fiscales interrumpir o desbaratar las actividades de grupos terroristas antes de que se concreten sus ataques o atentados.

G. Fase del juicio: cuestiones probatorias

1. Cuestiones relativas al uso de pruebas derivadas de fuentes de inteligencia

364. La integración de las actividades de inteligencia en los sistemas de justicia penal sigue siendo un problema fundamental para las autoridades encargadas de combatir el terrorismo. Como ya se dijo, en muchos casos de terrorismo las pruebas presentadas por la fiscalía proceden de fuentes de inteligencia. Un problema común que se presenta a las autoridades de todos los países al perseguir casos de terrorismo es el de cómo proteger la información confidencial contenida en los datos de inteligencia y, al mismo tiempo, cumplir con la obligación de garantizar a los acusados un juicio imparcial y una defensa eficaz, incluida la obligación de revelar a la defensa todas las pruebas esenciales de cargo.

2. Cuestiones relacionadas con la reunión y el uso de pruebas digitales

365. En los casos de terrorismo en que se hayan usado computadoras, dispositivos similares o Internet, las pruebas digitales serán una parte importante de las pruebas de cargo. En los casos en que un sospechoso no estaba físicamente presente en el lugar en que se cometió un acto terrorista, pero no obstante apoyó la realización del hecho mediante alguna acción en Internet, la presentación de pruebas que revelen sus “huellas digitales” puede constituir una demostración convincente de su complicidad y culpabilidad.

366. La experiencia enseña que el uso de pruebas digitales invariablemente da lugar a problemas de admisibilidad. Es fundamental, por tanto, tener mucho cuidado durante toda la investigación y todo el procesamiento de velar por que los métodos seguidos para su reunión, conservación, análisis y producción cumplan con las disposiciones pertinentes relativas a la prueba o al procedimiento, y que se ajusten a las buenas prácticas establecidas.

367. Las pruebas digitales pueden ser técnicamente complejas y contener términos y conceptos con los que no estén familiarizados el juez, el jurado o el tribunal que conozca del asunto. Los fiscales deben considerar, en estrecha coordinación con los investigadores y expertos, la mejor forma de presentar tales pruebas, de manera que sean fáciles de entender y resulten convincentes. En este sentido, podría ser útil el uso de diagramas y representaciones gráficas similares que indiquen el movimiento de los datos o los vínculos entre las computadoras y los usuarios.

368. Como parte de lo que debe probar la fiscalía en los juicios en que se ha usado, de una manera u otra, una computadora, es que, en el momento de la comisión de los hechos, era el acusado el usuario de la computadora, del dispositivo o del servicio de Internet empleado para la comisión del delito que se le imputa, y establecer los vínculos que demuestran ese hecho. Esto se puede hacer de varias formas: a) el acusado puede

confesar o admitir el hecho; b) su uso de la computadora se puede demostrar con pruebas indiciarias (por ejemplo, era la única persona presente en el lugar donde se encontraba la computadora o en el momento en que se usó, era el usuario registrado del hardware o software correspondiente, o había otra información en la computadora que era de conocimiento exclusivo del acusado); o c) el vínculo puede establecerse mediante el análisis del contenido del dispositivo o del servicio que presuntamente usó el acusado. Para lograrlo, el fiscal puede verse en la necesidad de presentar pruebas sobre las características específicas del material contenido en el dispositivo (por ejemplo, un documento) o un comentario hecho en una comunicación interceptada que solo se puede atribuir al acusado. Por último, la hora y fecha de los ficheros digitales pueden ser un método convincente, aunque no infalible, de vincular al acusado con el dispositivo correspondiente en el momento de la comisión del delito¹⁶⁵.

369. Aunque los detalles pueden variar, el enfoque general adoptado por los tribunales en muchos países a la hora de determinar la admisibilidad de las pruebas en los procesos penales se basa en la pertinencia y la fiabilidad: ¿es la prueba que una de las partes trata de aducir pertinente y fiable? En el caso de las pruebas digitales pertinentes, el problema para los fiscales en muchos casos será convencer al tribunal de la fiabilidad de estas, en lo que se refiere tanto al contenido como a los métodos usados para obtenerlas y presentarlas al juez. Para convencer a un tribunal de que las pruebas digitales son admisibles hay que probar a menudo la legalidad de los métodos seguidos para obtenerlas y asegurar su integridad desde el momento de la obtención hasta el de su presentación en juicio. Esto se conoce como la “cadena de custodia” o “cadena de pruebas”: los mecanismos, tanto operacionales como jurídicos, para preservar la integridad de las pruebas. En la mayoría de los países, existen estrictas normas jurídicas relativas a la cadena de custodia, que requieren que los elementos de prueba se registren, centralicen y sellen de inmediato, y protejan de la contaminación mientras está pendiente el juicio, todo ello, en algunos casos, bajo la supervisión de un funcionario judicial.

370. En los casos de terrorismo en que se hayan obtenido y vayan a usarse comunicaciones interceptadas o pruebas forenses digitales, los fiscales deben asegurarse, trabajando en estrecha colaboración con los organismos de inteligencia o de aplicación de la ley, o ambos, de que estas fueron obtenidas y conservadas de conformidad con la ley, y se presentarán en juicio de manera acorde con los requisitos probatorios de la jurisdicción en que finalmente hayan de utilizarse. La reunión y producción de datos digitales como pruebas admisibles, especialmente cuando los tiene un sospechoso, o un tercero, situado a distancia, en otras jurisdicciones, es una tarea difícil, tanto para los investigadores como para los fiscales. Además de las complicaciones técnicas de la obtención de los datos requeridos y la preservación de su integridad, la necesidad en algunas situaciones de confiar en la cooperación de los organismos extranjeros de inteligencia, de ejecución de la ley o de procuraduría, que actúan con arreglo a diferentes leyes y procedimientos que regulan la reunión y el uso de esos datos, puede hacer que tales procedimientos sean largos y exijan gran cantidad de recursos.

¹⁶⁵Departamento de Justicia de los Estados Unidos, Oficina de Programas de Justicia, Instituto Nacional de Justicia, *Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors* (2007), cap. 4, art. IV. Se puede consultar en www.ncjrs.gov/pdffiles1/nij/211314.pdf.

371. En las investigaciones en que la reunión de datos digitales se efectúa en su totalidad en una sola jurisdicción, las cuestiones relativas a su admisibilidad como prueba tienden a centrarse en la legalidad de su obtención y el posterior manejo y preservación (es decir, la cadena de custodia o de prueba). Como siempre, es necesario asegurarse de que el fundamento jurídico de su obtención, el examen forense, la preservación y producción estén en plena consonancia con las normas y los procedimientos aplicables a la admisibilidad de las pruebas.

372. En el caso de los datos digitales obtenidos en una o más jurisdicciones para su uso en una acción penal en una jurisdicción diferente, la situación es mucho más complicada y requiere especial atención por parte de los investigadores y fiscales.

373. Tan pronto como sea posible después de haber determinado que los datos pertinentes para la investigación están en poder de alguien situado en una jurisdicción extranjera, los investigadores y los fiscales deben explorar los medios tanto oficiosos como oficiales para la obtención y conservación de esos datos con fines probatorios. Siempre que sea posible y factible, deben preferirse los canales oficiosos para obtener los datos que en definitiva se presentarán como pruebas, siempre que los métodos por los que se reúnan, conserven y transmitan al país receptor cumplan con las normas y procedimientos probatorios aplicables. Para la obtención de estos datos, los investigadores pueden verse en la necesidad de solicitar a sus homólogos extranjeros que obtengan una orden de registro e incautación o de considerar el uso de otros medios (por ejemplo, páginas web accesibles al público) o la presentación de testigos voluntarios extranjeros.

374. Una causa de Alemania, que terminó en 2009 y en la que se procesó con éxito a cuatro miembros de la Unión de la Yihad Islámica, ilustra la magnitud y complejidad de muchas investigaciones y enjuiciamientos de terrorismo. En este caso se realizó una investigación que duró nueve meses; participaron más de 500 agentes de policía; se acumuló un sinnúmero de horas de interceptación y vigilancia electrónicas y se reunió una multitud de elementos de prueba; se necesitó, por tanto, una extensa cooperación internacional entre las autoridades alemanas y sus homólogos en Turquía y los Estados Unidos. La magnitud y complejidad del caso ponen de relieve los enormes recursos que se necesitan a veces para llevar a cabo investigaciones y enjuiciamientos y las ventajas del enfoque de equipo, con frecuencia indispensable.

Fritz Gelowicz, Adem Yilmaz, Daniel Schneider y Atilla Selek

En septiembre de 2007, después de una intensa investigación, las autoridades alemanas, que actuaban basándose en inteligencia recibida de sus homólogos de los Estados Unidos, detuvieron a cuatro miembros de la Unión de la Yihad Islámica (llamada a veces la "célula de Sauerland"), que se encontraban en las etapas finales de la preparación de una serie de atentados con bombas en varios lugares públicos de Alemania. Algunos de los objetivos eran bares y discotecas en distintos lugares públicos de Munich, Colonia, Francfort, Dusseldorf y Dortmund, así como en la base aérea de los Estados Unidos en Ramstein. El volumen total de material explosivo que los acusados creían haber conseguido (en realidad, había sido reemplazado subrepticamente por las autoridades con una sustancia inocua) era enorme, potencialmente con una fuerza superior a la de los atentados terroristas de Madrid (2004) y Londres (2005).

Tres de los acusados —Gelowicz, Schneider y Selek— eran nacionales alemanes; el cuarto, Yilmaz, era de nacionalidad turca. En el transcurso de varios meses, los acusados adquirieron de fuentes legítimas 780 kg de agua oxigenada. El 4 de septiembre de 2007, las autoridades detuvieron a los acusados cuando se encontraban reunidos en una casa de vacaciones situada en el Sauerland, una región de Alemania, donde habían comenzado a mezclar el agua oxigenada con otras sustancias para darle un efecto explosivo. (Sin que lo supieran los acusados, las autoridades habían sustituido previamente la solución de agua oxigenada por otra inocua, de menor concentración).

En agosto de 2008, los fiscales federales presentaron acusaciones en contra de Gelowicz, Schneider y Yilmaz. Selek fue extraditado de Turquía en noviembre de 2008, en respuesta a un pedido de extradición en virtud del Convenio Europeo sobre Extradición, y fue acusado en diciembre de 2008. Los cargos eran de confabularse para cometer un homicidio, realizar actos preparatorios de un atentado con explosivos y pertenecer a una organización terrorista.

El juicio de los cuatro acusados se inició en abril de 2009 y duró tres meses, hasta que los acusados decidieron admitir los cargos. La cantidad de pruebas que la fiscalía tenía la intención de presentar era enorme: incluía 521 carpetas de anillas (suficientes para llenar un estante de 42 metros de largo) y 219 testigos. Gran parte de las pruebas de cargo provenían de la monitorización y vigilancia electrónicas intensivas realizadas por las autoridades alemanas durante la investigación. Las técnicas electrónicas de investigación incluían el uso de escuchas telefónicas de diálogos entre los acusados y dispositivos de escucha plantados en vehículos y en la casa donde se reunían para fabricar explosivos con el agua oxigenada, así como la interceptación de los mensajes electrónicos intercambiados. La fiscalía se había propuesto originalmente reunir gran cantidad de pruebas digitales; sin embargo, había habido claras señales de que los sospechosos, mientras conspiraban, habían tomado precauciones contra la vigilancia o monitorización. Durante los nueve meses que duró la investigación, las autoridades tropezaron con una serie de problemas técnicos. Por ejemplo, los acusados se habían comunicado usando borradores de mensajes electrónicos (es decir, abriendo y leyendo borradores de mensajes en cuentas de correo electrónico) para soslayar las escuchas telefónicas de los organismos de aplicación de la ley, y habían utilizado conexiones inalámbricas no protegidas de redes locales de personas inocentes y comunicaciones cifradas a través de proveedores de servicios de telefonía de voz por Internet (VoIP) (Skype, por ejemplo).

Considérese el caso de Gelowicz, presunto cabecilla del grupo: Gelowicz utilizó el acceso aleatorio a Internet a través de redes locales privadas, residenciales, no protegidas; empleó por lo menos 14 cuentas de correo electrónico diferentes; cambió las placas de vehículos y se sirvió de un escáner de la policía para monitorizar las comunicaciones de radio de la policía. Gelowicz había protegido los datos de su computadora por medio de cifrado, que los expertos forenses intentaron descifrar y acceder infructuosamente. Gelowicz finalmente dio la clave del cifrado, pero los investigadores solo encontraron rastros de datos triturados.

Durante el juicio, la defensa impugnó la validez del proceso, cuestionando el fundamento de la investigación, que, en su opinión, era intrínsecamente defectuoso, por basarse en inteligencia reunida por los Estados Unidos, que, según afirmó, incluía la monitorización electrónica de las comunicaciones de los acusados, que era ilegal y había sido proporcionada en violación de sus derechos con arreglo a la Constitución de Alemania.

El 4 de marzo de 2010, los cuatro acusados fueron declarados culpables de todos los cargos y sentenciados: Gelowicz y Schneider a 12 años de prisión, Yilmaz a 11 años de prisión y Selek a 5 años de prisión.

3. Cuestiones relacionadas con el uso de pruebas extranjeras

375. Los principios y procedimientos jurídicos relacionados con la obtención y admisibilidad de las pruebas en los procesos penales suelen ser diferentes en distintas jurisdicciones. Una de las mayores dificultades que enfrentan los investigadores y fiscales en cualquier investigación y proceso penal de carácter transfronterizo (tanto en el país requerido como en el requirente) es asegurarse de que las pruebas necesarias se reúnan, preserven, transmitan y presenten de conformidad con los procedimientos y las normas probatorias aplicables por ley en las jurisdicciones respectivas para que sean admisibles en juicio en el lugar en que se lleve a cabo.

376. El proceso de “mediar” diferentes aspectos de la prueba entre países puede ser complejo y llevar mucho tiempo, pero es un factor crítico para lograr el éxito del procesamiento. Las pruebas obtenidas o presentadas por métodos que sean jurídicamente deficientes serán impugnadas en juicio, casi con certeza, por los abogados de la defensa.

377. Un ejemplo útil, que pone de relieve los tipos de problemas que pueden surgir en este contexto, es la causa belga de *Malika el Aroud y otros*, que está relacionada con las actividades de un grupo de personas acusadas de participar en el establecimiento y la administración de varios sitios web que usaban para difundir propaganda terrorista e información útil a los terroristas, y de foro para comunicarse entre sí. Varios de los acusados vivían en Bélgica, pero el sitio web principal en que llevaban a cabo sus actividades (minbar-sos.com) se hospedaba en el Canadá.

Malika el Aroud y otros

Introducción

En diciembre de 2008, después de investigaciones largas, intensas y complejas, coordinadas entre los organismos de aplicación de la ley, de inteligencia y las autoridades judiciales de Francia, Bélgica, Suiza, Italia, Turquía, los Estados Unidos y el Canadá, varias personas de quienes se sospechaba que tenían vínculos con la organización terrorista Al-Qaida fueron detenidas y acusadas en Francia y Bélgica, con una serie de cargos que incluían el de participar como miembro en un grupo terrorista, financiar el terrorismo y suministrar información y recursos materiales a un grupo terrorista.

Para realizar los presuntos actos que constituían la base de estos cargos, los sospechosos habían hecho amplio uso de Internet. La investigación de sus actividades consistió en una vigilancia electrónica compleja, escuchas telefónicas y otras formas de monitorización por parte de los organismos de inteligencia y de aplicación de la ley. Para llevar el caso a feliz término, fue necesaria la cooperación, tanto oficial como oficiosa, de las autoridades de varias jurisdicciones distintas.

Este caso es un buen ejemplo de cooperación en procesos penales de terrorismo, con aspectos relacionados con Internet, establecida con pleno éxito entre las autoridades nacionales de todos los Estados participantes, y pone de relieve muchos aspectos de las buenas prácticas mencionadas en la presente publicación. Estos aspectos se tratan en los capítulos V y VI, sobre la cooperación internacional y el proceso penal.

La causa, que estaba vinculada con otras causas en varios países, giraba principalmente en torno a las actividades de Malika el Aroud, nacional belga de origen marroquí, y su marido, Moez Garsallaoui, de nacionalidad tunecina. Ambos participaban activamente en la difusión de propaganda yihadista radical y en el reclutamiento, la organización, dirección y financiación de un grupo de jóvenes procedentes de Bélgica y Francia para que lucharan como yihadistas en el Afganistán y otros lugares.

Si bien algunas de estas actividades se realizaron usando otros métodos, la pareja se sirvió de Internet en gran medida para llevar adelante sus acciones y para comunicarse. Además de El Aroud y Moez Garsallaoui (que, junto con un cómplice, Hicham Beyayo, fue juzgado en ausencia), los otros acusados sometidos a juicio fueron Ali el Ghanouti, Said Arissi, Trefois Jean-Christophe, Bastin Abdulaziz, Mohamed el-Amin y Bastin Hicham Bouhali Zrioul.

La causa belga guarda estrecha relación tanto con una causa de Francia, en que los acusados Walid Othmani Hamadi Aziri, Samira Ghamri Melouk, Berrached Hicham y Youssef el Morabit fueron juzgados y condenados ante el Tribunal de Grande Instance de París^a, como con una investigación y enjuiciamiento en Italia de Bassam Avachi y Gendron Raphaël.

Antecedentes

En agosto de 2007, las autoridades belgas recibieron información de sus homólogos franceses relativa a las actividades en el sitio web Minbar SOS (hospedado en el Canadá), porque sospechaban que se estaba utilizando para difundir propaganda que incitaba a la yihad salafista contra Francia. El sitio estaba presuntamente administrado por El Aroud y Garsallaoui. A medida que se amplió la investigación, se encontraron otros sitios web similares.

Las autoridades sospechaban que El Aroud y Garsallaoui, actuando de consuno a través del sitio, buscaban y reclutaban personas en Bélgica para luchar en el Afganistán. El Aroud publicó arengas incendiarias que incitaban a los jóvenes a unirse a la yihad.

Malika el Aroud y Moez Garsallaoui

Malika el Aroud y Garsallaoui Moez ya eran bien conocidos por los organismos de lucha contra el terrorismo de Europa. En 2003, El Aroud había sido juzgada y absuelta por un tribunal de Bélgica por su presunta participación en una red de apoyo logístico yihadista utilizada en el asesinato de un líder de la resistencia contra los talibanes en septiembre de 2001. Uno de los dos atacantes había sido el primer marido de El Aroud.

En 2007, El Aroud fue procesada en Suiza, junto con Garsallaoui, su segundo marido, por proporcionar "apoyo a una organización delictiva" y por "incitación pública a la violencia y la delincuencia" a través de los diferentes sitios web que ambos habían establecido en Suiza. Fue declarada culpable y condenada a una pena de seis meses de prisión suspendida por el Tribunal Penal Federal de Bellinzona.

El 21 de diciembre de 2007, El Aroud fue detenida en Bélgica porque se sospechaba que había tratado de ayudar a un reo a escapar de la prisión, Nizar T.; pero fue puesta en libertad, después de 24 horas, por falta de pruebas. En 2004, Nizar T. había sido condenado por un tribunal en Bélgica a 10 años de prisión por haber preparado un atentado terrorista contra la base militar de los Estados Unidos en Kleine-Brogel en 2007. Esta detención se produjo mientras se investigaban sus actividades sospechosas en Minbar SOS.

Los sitios web

Los sitios web establecidos por El Aroud, incluido Minbar SOS, se usaban como plataforma para publicar propaganda (videos y fotografías), difundir libros y publicaciones y comunicarse entre sí. A cada uno de los miembros se les proporcionaba un nombre de usuario o seudónimo y una dirección electrónica para que pudieran intercambiarse mensajes privados, a veces cifrados, en salas de charla privadas que se hospedaban en los sitios. Estos contenían instrucciones, datos de inteligencia, propaganda y llamamientos constantes a una yihad masiva. Parte del material contenía referencias claras a los dirigentes de Al-Qaida e incluía anuncios de ataques contra las tropas estadounidenses en el Iraq.

Se publicaban mensajes con amenazas explícitas (por ejemplo, un mensaje titulado: "Contra el terrorismo francés en el Afganistán, solamente una solución"), junto con un plano de la red de trenes regionales (RER) de París, en que se habían señalado algunas de las estaciones principales con símbolos de radiactividad o de contaminación biológica. En algunos mensajes se daban instrucciones explícitas sobre cómo transferir fondos a miembros de la yihad. A finales de 2008, el sitio principal, Minbar SOS, contaba con más de 1.400 abonados.

Como parte de una investigación conjunta, las autoridades belgas y francesas interceptaron comunicaciones de los sitios web, mensajes electrónicos y llamadas telefónicas, y monitorizaron y rastrearon las corrientes de fondos. Sin embargo, aunque los organismos de seguridad belgas monitorizaban muy de cerca la actividad de Internet en la página web Minbar SOS destinada a reclutar combatientes para el Afganistán, era poco lo que podían hacer para evitar que El Aroud administrara el sitio, debido a la fuerte protección de la libertad de expresión que ofrece el derecho belga.

El tribunal francés, donde finalmente se realizó el juicio relacionado con la causa en ese país, señaló, refiriéndose a los sitios web:

La actividad en estos sitios web no puede ser analizada como una simple búsqueda de información o inteligencia, sino que, por el contrario, debe verse como una participación consciente en una empresa o misión terrorista.

Además, en los testimonios prestados en juicios posteriores, los procesados Arissi y Beyayo Hicham declararon, respectivamente, lo siguiente: "Me considero una víctima de la propaganda de Internet" y "los sitios web como Ribaati y Minbar SOS influyen en la gente como yo, que fuimos a luchar", lo que ilustra la fuerte influencia que tuvieron las actividades del sitio en algunas personas.

En una rara entrevista, para un artículo que apareció en *The New York Times* el 28 de mayo de 2008, El Aroud se describió a sí misma como "una guerrera santa de Al-Qaida. Ella insiste (...) en que no tenía ninguna intención de tomar las armas ella misma. Más bien, acicateaba a los hombres musulmanes a luchar y a las mujeres a sumarse a la causa. 'Mi misión no es poner bombas; eso es ridículo ... Tengo un arma. Es la escritura. Es la palabra. Esa es mi yihad. Se pueden hacer muchas cosas con la palabra. También la palabra es una bomba'"^b.

Viajes de reclutas a las Zonas Tribales de Administración Federal del Pakistán

Además de las actividades realizadas a través de los sitios web, Garsallaoui recorría los barrios de inmigrantes de Bruselas para reclutar gente en persona. Hicham Beyayo, uno de los detenidos en la causa, de 23 años de edad, nacional belga de origen marroquí, que era uno de los administradores del sitio Minbar SOS antes de viajar al Pakistán, admitió haber sido reclutado de esa manera.

La labor de reclutamiento de Garsallaoui no se limitaba a Bélgica, sino que también reclutó a dos abonados franceses de Minbar SOS. Uno de esos reclutas, que viajó a las Zonas Tribales de Administración Federal del Pakistán y fue detenido más tarde, dijo que los llamamientos de Minbar SOS a la “yihad” eran “incesantes” y que la propaganda de videos que había visto en el sitio lo habían impulsado a ofrecerse como voluntario.

En diciembre de 2007, Garsallaoui y seis reclutas, incluidos Hicham Beyayo, Ali el Ghanouti y Y. Harrizi, viajaron a las Zonas Tribales de Administración Federal del Pakistán a través de Turquía y de la República Islámica del Irán. El grupo se quedó allí hasta el segundo semestre de 2008. Mientras estuvo en las Zonas, Garsallaoui se mantuvo en contacto permanente con El Aroud por medio del correo electrónico y a veces por Skype. Además de enviar fotografías y otro material de propaganda, publicaba declaraciones y periódicamente visitaba los foros de Minbar SOS.

El 26 de septiembre de 2008, Garsallaoui publicó una declaración en línea, en Minbar SOS, en la que exhortaba a que se realizaran ataques en Europa: “La solución, hermanos y hermanas, no son fatwas sino booooooms”, decía el mensaje.

Las detenciones

Durante un período de varios meses, en el segundo semestre de 2008, algunos de los sospechosos comenzaron a regresar a Bélgica. Se puso en estado de alerta a los servicios de seguridad belgas después de que El-Ghanouti y Harrizi regresaron de las Zonas Tribales de Administración Federal, y el 4 de diciembre de 2008 también Beyayo regresó a Bélgica.

Se dieron diferentes razones para explicar por qué los reclutas volvieron a Bélgica en ese momento. Algunos de los sospechosos sostuvieron que no estaban satisfechos con el trato recibido y las condiciones en que se encontraban en las Zonas Tribales de Administración Federal, que incluían restricciones a sus posibilidades de participar en la yihad, y negaron la existencia de una “célula durmiente” destinada a llevar a cabo atentados en Bélgica. Sin embargo, las autoridades belgas consideraron que las comunicaciones interceptadas proporcionaban un fundamento sólido para sospechar que el grupo podía estar en las etapas finales de la planificación de un atentado terrorista suicida (tal vez usando a Hicham Beyayo) en Bélgica, lo que exigía una acción inmediata.

El 11 de diciembre, una semana después del regreso de Beyayo, las autoridades belgas allanaron 16 locales en Bélgica y detuvieron a nueve sospechosos, entre ellos El Aroud, Garsallaoui y Beyayo. En Francia e Italia se llevaron a cabo operaciones similares.

El proceso penal

Bélgica

En el juicio, los abogados de la defensa impugnaron diversos aspectos de los argumentos de la fiscalía, tanto por cuestiones de procedimiento como por la admisibilidad de ciertas pruebas, incluidos los datos relacionados con Internet obtenidos a título oficioso por el FBI de un proveedor de servicios de Internet con sede en los Estados Unidos. Los problemas relacionados con esta clase de pruebas se tratan con mayor detenimiento más adelante en la presente publicación.

Las autoridades de Marruecos habían entrevistado a Beyayo el 20 de mayo de 2008. Sus abogados defensores argumentaron que se había violado su derecho a tener un juicio imparcial, basándose en sospechas de que las autoridades marroquíes habían torturado a los detenidos por sospechas de que habían cometido actos de terrorismo. El tribunal rechazó esos argumentos.

El proceso penal

Bélgica

En el juicio, los abogados de la defensa impugnaron diversos aspectos de los argumentos de la fiscalía, tanto por cuestiones de procedimiento como por la admisibilidad de ciertas pruebas, incluidos los datos relacionados con Internet obtenidos a título oficioso por el FBI de un proveedor de servicios de Internet con sede en los Estados Unidos. Los problemas relacionados con esta clase de pruebas se tratan con mayor detenimiento más adelante en la presente publicación.

Las autoridades de Marruecos habían entrevistado a Beyayo el 20 de mayo de 2008. Sus abogados defensores argumentaron que se había violado su derecho a tener un juicio imparcial, basándose en sospechas de que las autoridades marroquíes habían torturado a los detenidos por sospechas de que habían cometido actos de terrorismo. El tribunal rechazó esos argumentos.

Actividades de Bryan Neal Vinas (Estados Unidos)

En enero de 2009, un nacional de los Estados Unidos, Bryan Neal Vinas, viajó al Afganistán, donde intentó matar a soldados estadounidenses durante un ataque con cohetes de Al-Qaida contra una base militar. Más tarde fue detenido y enviado de regreso a los Estados Unidos, donde fue acusado de confabularse para asesinar a nacionales de los Estados Unidos, proporcionar apoyo material a Al-Qaida y recibir entrenamiento militar de este grupo. Vinas se declaró culpable y fue condenado a una pena de prisión.

Las autoridades belgas que enjuiciaron a Beyayo, cómplice de El Aroud, presentaron pruebas del juicio de Vinas para demostrar el alcance de sus actividades y la participación de estos acusados en la red de Al-Qaida. En sus declaraciones, Vinas había admitido haber conocido a algunos de los reclutas belgas. La defensa impugnó la admisibilidad de la prueba por una serie de motivos, pero el tribunal rechazó esos argumentos.

Resultado del juicio

Después del juicio, el 10 de mayo de 2010, el Tribunal de Primera Instancia de Bruselas dictó las sentencias de nueve acusados que habían sido enjuiciados por cargos diferentes, que correspondían a tres categorías: A, B y C.

Los cargos de las categorías A y C, respectivamente, se referían a la participación como cabecillas en un grupo terrorista y a la participación en actividades de un grupo terrorista, que incluían el suministro de información o medios materiales, o de cualquier forma de financiación de la actividad de un grupo terrorista, a sabiendas de que dicha participación ayudaría al grupo a cometer un crimen o delito.

Los cargos de la categoría B incluían la comisión de delitos o la prestación de asistencia en la comisión de delitos por medio de donaciones, promesas, amenazas, abuso de autoridad o de poder, planes o conjuraciones con la intención de cometer delitos contra las personas o bienes con el fin de causar daños graves, así como delitos que, por su carácter o contexto, podían causar graves daños a un país o a una organización internacional y que fueron cometidos intencionalmente con el fin de intimidar seriamente a una población u obligar indebidamente a las autoridades públicas o a una organización internacional a tomar medidas, o de desestabilizar gravemente o destruir las estructuras fundamentales políticas, constitucionales, económicas o sociales de un país o de una organización internacional.

Las penas impuestas por los cargos de la categoría A fueron las siguientes:

- Malika el Aroud: ocho años de prisión y multa de 5.000 €
- Moez Garsallaoui: ocho años de prisión y multa de 5.000 € (en ausencia)
- Hicham Beyayo: cinco años de prisión y multa de 1.000 € (en ausencia)

Las condenas en virtud de los cargos de la categoría B fueron las siguientes:

- Ali el Ghanouti: absuelto
- Said Arissi: absuelto

Las penas en virtud de los cargos de la categoría C fueron las siguientes:

- Ali el Ghanouti: tres años de prisión y multa de 500 €
- Said Arissi: 40 meses de prisión y multa de 500 €
- Hicham Bouhali Zrioul: cinco años de prisión y multa de 2.000 € (en ausencia)
- Abdulaziz Bastin: 40 meses de prisión y multa de 500 €
- Mohamed el Amin-Bastin: 40 meses de prisión y multa de 500 €
- Jean-Christophe Trefois: absuelto

Francia

En Francia, los cinco sospechosos (todos nacionales franceses de ascendencia norteafricana) fueron juzgados ante el Tribunal de Grande Instance de París. Walid Othmani, Aziri Hamadi, Samira Ghamri Melouk, Berrached Hicham y Youssef el Morabit habían sido acusados de varios delitos: financiación del terrorismo, confabulación para cometer un acto terrorista y participación en un grupo formado con el propósito de preparar un acto terrorista tipificado en el artículo 421-1 del Código Penal francés.

Italia

Bassam Ayachi y Raphael Gendron (ambos nacionales franceses) fueron acusados por las autoridades italianas de asociación delictiva con el objeto de cometer los actos de terrorismo previstos en el artículo 207 bis, párrafo 1, del Código Penal italiano, que impone una pena de 7 a 15 años de prisión para el que sea declarado culpable de integrar, promover, organizar, administrar o financiar grupos que tienen la intención de llevar a cabo actividades violentas para lograr fines terroristas o la subversión de la estructura democrática del Estado, y una pena de prisión de 5 a 10 años para los que se asocien a dichos grupos.

En el juicio se demostró que existían vínculos entre los dos acusados y algunos de los procesados del juicio belga, así como elementos de prueba comunes a ambos, que incluían un DVD con una nota de suicidio, escrita por uno de los sospechosos belgas.

El 3 de junio de 2011, Ayachi y Gendron fueron condenados a ocho años de prisión.

Fuente: Eurojust, *Terrorism Convictions Monitor*, núm. 8, septiembre de 2010.

^aSentencia del 18 de febrero de 2011 (No. d'affaire 1015239014).

^bVéase "Al Qaeda warrior uses Internet to Rally Women", *The New York Times* (28 de mayo de 2008). Se puede consultar en www.nytimes.com/2008/05/28/world/europe/28terror.html?_r=1&pagewanted=all.

378. En el caso de El Aroud, la fiscalía presentó como pruebas datos de Internet relacionados con anuncios y discusiones en salas de charla. En el caso de los mensajes electrónicos (estos últimos enviados desde cuentas mantenidas por Yahoo y Microsoft), los datos se encontraban en servidores de los Estados Unidos. Previa solicitud oficiosa de asistencia, las autoridades belgas recibieron (en dos semanas) un CD del FBI que contenía los datos relativos a las cuentas de correo electrónico especificadas y otras cuentas conexas. El FBI dejó constancia de que habían sido proporcionados voluntariamente por Yahoo y Microsoft, según lo permiten las disposiciones de la Ley Patriota de los Estados Unidos.

379. La defensa impugnó la admisibilidad de las pruebas, afirmando que los procedimientos seguidos para reunirlos, transmitirlos y presentarlos eran ilegales, ya que se habían obtenido sin una orden de registro y, además, porque el trámite oficioso empleado no se había ajustado a los métodos habituales de intercambio internacional de información judicial, lo que contravenía el artículo 7, párrafo 1, de la ley belga de 9 de diciembre de 2004, sobre asistencia judicial recíproca internacional en materia penal.

380. El Tribunal rechazó este argumento, sosteniendo que: *a)* el intercambio de información no se había producido en el marco de la asistencia judicial recíproca; *b)* no se había designado ningún juez de instrucción para la causa en el momento de los hechos, que investigaba la policía a título oficioso; y *c)* el procedimiento empleado se justificaba por el carácter urgente de las circunstancias (es decir, el descubrimiento de una nota de suicidio en el sitio web Minbar SOS por uno de los sospechosos, lo que hacía pensar que era inminente un ataque en suelo francés orquestado por Malika el Aroud y sus asociados). El Tribunal sostuvo que por esos motivos el juez federal había concluido fundadamente que la cooperación policial de emergencia se basaba en lo dispuesto en el artículo 15, párrafo *b)*, del Convenio Internacional para la represión de los atentados terroristas cometidos con bombas (1997)¹⁶⁶, que prevé el “intercambio de información precisa y corroborada, de conformidad con su legislación interna, y la coordinación de medidas administrativas y de otra índole adoptadas, según proceda, para impedir que se cometan los delitos previstos en el artículo 2”¹⁶⁷.

381. Por último, el Tribunal declaró que, puesto que la base jurídica de la información transmitida a la policía belga por las autoridades estadounidenses era válida, dicha información podía de hecho ser utilizada por las autoridades judiciales belgas. El Tribunal añadió que el análisis relativo a las direcciones de correo electrónico (o la mayoría de ellas) con base en los Estados Unidos se había incluido en el expediente judicial en respuesta a una comisión rogatoria ejecutada en Francia¹⁶⁸.

382. Esta causa pone de manifiesto la cuidadosa atención que hay que prestar, durante la fase de la investigación de casos relacionados con el uso de pruebas extranjeras, a los métodos empleados en la reunión y transmisión de dichas pruebas. Esto refuerza

¹⁶⁶Naciones Unidas, *Treaty Series*, vol. 2178, núm. 38349.

¹⁶⁷Eurojust, *Terrorism Conviction Monitor*, núm. 8, septiembre de 2010.

¹⁶⁸Ibid.

la importancia, subrayada por varios participantes en la reunión del grupo de expertos, de que los fiscales queden integrados desde un principio en la investigación para detectar y resolver los posibles problemas probatorios antes del juicio.

383. En la causa *Namouh* (Canadá), la acusación tuvo que presentar en juicio pruebas reunidas por un agente de policía austríaco, lo que resultó problemático. Según la legislación austríaca, las pruebas presentadas por un agente de policía pueden ser admitidas como pruebas en la forma de una declaración por escrito. Sin embargo, este no es el caso con arreglo al derecho canadiense, que generalmente excluye el testimonio indirecto y requiere la comparecencia en juicio para prestar testimonio oral. Con el fin de facilitar la presentación de las pruebas del agente, los fiscales canadienses tuvieron que mantener un estrecho contacto con la policía y los fiscales austríacos para explicar las normas probatorias aplicables conforme a la ley canadiense, así como con la defensa, para facilitar un acuerdo de que las pruebas del agente se podían presentar en forma escrita.

4. *Uso de pruebas periciales*

384. En los casos relacionados con el terrorismo suele suceder que los fiscales tengan que presentar pruebas periciales para demostrar algún aspecto especial de un caso. Sin embargo, la gama de posibles problemas que puede crear este tipo de pruebas es sumamente amplia. De los enjuiciamientos ya realizados relacionados con actos de terrorismo mediados por Internet, es posible determinar en términos generales cuáles son las esferas en que los investigadores o fiscales pueden verse en la necesidad de prestar atención a este problema.

385. La informática y la tecnología de las comunicaciones continúan evolucionando a un ritmo muy rápido, volviéndose cada vez más complejas y especializadas. Es muy probable que los fiscales puedan necesitar el testimonio de varios peritos para explicar aspectos técnicos diferentes, pero relacionados, de los sistemas informáticos o de comunicaciones o actividades conexas en el curso del mismo procedimiento, especialmente cuando hay pruebas de que un sospechoso ha usado un equipo, dispositivo o servicio de Internet determinado¹⁶⁹.

386. Además de las pruebas relacionadas con el examen forense de datos informáticos en casos de presunta participación en grupos terroristas o de presunta prestación de apoyo material a estos, o de incitación, reclutamiento o adiestramiento, puede necesitarse testimonio pericial sobre las ideologías, los objetivos y las actividades de las estructuras orgánicas de determinados grupos terroristas o de determinadas personas.

387. Por lo general, los casos que requieren el testimonio de peritos abarcan tres etapas o fases: *a)* determinación clara de cuáles son los problemas (y su alcance) que requieren un dictamen pericial, *b)* selección de un experto cualificado, y *c)* necesidad de asegurarse de que el experto cualificado utilice medios admisibles¹⁷⁰.

¹⁶⁹Walden, *Computer Crimes and Digital Investigations*, pág. 383.

¹⁷⁰Instituto Nacional de Justicia, *Digital Evidence in the Courtroom*, cap. 3, secc. III. E.

a) *Determinación clara de cuáles son los problemas*

388. Los fiscales, trabajando en estrecha coordinación con los investigadores, deben determinar cuanto antes qué problemas exigirán, a su juicio, testimonio pericial y contratar a los expertos para que hagan los análisis necesarios, proporcionándoles una orientación clara sobre los elementos clave de la prueba.

b) *Selección de un experto cualificado*

389. Al seleccionar a los peritos que prestarán testimonio sobre aspectos especializados de las pruebas en los juicios de terrorismo, los fiscales deben considerar si han de contratar a expertos gubernamentales o no gubernamentales. Si bien el uso de expertos gubernamentales es permisible y ofrece algunas ventajas, ello podría no ser aconsejable si es probable que en las actuaciones previas al juicio los requisitos de revelación o la repregunta en juicio de esos testigos por la defensa hicieran salir a luz las fuentes confidenciales de inteligencia y los métodos mediante los cuales se obtuvo la información en que basan sus opiniones. Para evitar este posible problema, los fiscales podrían preferir recurrir a peritos académicos o no gubernamentales, que normalmente basan su testimonio en información de dominio público, que puede ser revelada libremente, sin el riesgo de comprometer las fuentes o los métodos de los servicios de inteligencia¹⁷¹.

390. Un buen ejemplo de un caso en que la fiscalía contrató a expertos no gubernamentales es el de Namouh, en que se llamó a declarar a dos testigos para que explicaran los objetivos y las modalidades de actuación del Frente Mundial de Medios de Información Islámicos (GIMF). En el párrafo 394 *infra* se describen los antecedentes de este testimonio.

391. La selección de un experto adecuado, sobre todo en campos altamente especializados, puede ser un problema serio para las jurisdicciones de menor desarrollo. Los fiscales, en colaboración con los investigadores, deberían adoptar un enfoque proactivo y prudente, y tratar de explorar todas las vías para obtener los servicios (cuando sea posible) de los peritos necesarios, adecuadamente cualificados, a nivel nacional, pero, en caso necesario, deberán tomar medidas para contratar a un testigo adecuado a nivel internacional.

c) *Necesidad de asegurarse de que el experto use medios admisibles*

392. La necesidad de que los testigos periciales de cargo sigan y observen las buenas prácticas reconocidas en todo examen o análisis que emprendan en el ámbito específico en que se los ha llamado a declarar es, sin duda, muy importante. Esto es particularmente cierto de cualquier análisis forense que realicen con el propósito de fundamentar las opiniones que ofrecerán como parte de las pruebas presentadas por la fiscalía. Los

¹⁷¹ Oficina de las Naciones Unidas contra la Droga y el Delito, *Compendio de casos relativos a la lucha contra el terrorismo*, párr. 194.

investigadores y fiscales deberán considerar, en la primera oportunidad posible, si hará falta testimonio pericial en algún aspecto especializado de la acusación y, de ser así, deberán consultar y contratar a peritos idóneos sin pérdida de tiempo para asegurarse de que la base probatoria del testimonio pericial se preserve en una forma admisible.

393. En algunos casos, especialmente los relacionados con la tecnología informática, las pruebas pueden ser técnicamente complejas, y los fiscales y peritos deben considerar formas innovadoras de presentar en el juicio esas pruebas a los jueces, jurados u otros jueces de hecho de manera clara, fácil de entender y convincente. Por ejemplo, el uso de una representación gráfica del diseño del sistema o del tráfico de datos, en lugar de presentar solo el testimonio oral, podría ayudar al juez de hecho a entender mejor los aspectos técnicos relacionados con los sistemas informáticos o de comunicaciones. Evidentemente, también es importante que el fiscal tenga un sólido conocimiento práctico del tema en particular para poder explicar los términos y conceptos al juez, jurado o tribunal y presentar de manera eficaz los argumentos de la acusación.

394. El caso canadiense de *Namouh* exigió un extenso uso del testimonio pericial (prestado por un perito de la Real Policía Montada del Canadá especializado en ciencia forense digital) sobre cuestiones relacionadas con las pruebas digitales. Estas consistían básicamente en el presunto uso por el acusado de una computadora (incautada en su domicilio) y el uso conexo de Internet, incluidas su participación en foros de discusión en línea, la carga de material en sitios web y las comunicaciones con otro cómplice situado en Austria. Este testimonio pericial detallado sobre temas forenses digitales era necesario para convencer al tribunal de que era el acusado quien había operado las computadoras desde las que se habían enviado los mensajes incriminatorios, así como para describir las ideologías y los métodos del GIMF, el frente mundial en que el acusado era participante activo.

395. Parte de la defensa de *Namouh* se centró en socavar este aspecto de los argumentos de la acusación. Afirmó en efecto que, debido a la falibilidad fundamental de Internet, ningún perito podía utilizarla de forma fiable como fuente de información para opinar sobre la actividad del GIMF y otros grupos terroristas. En particular, la defensa afirmó que los peritos no podían determinar de manera fiable si los anuncios publicados en foros de charla de Internet, y otras formas de comunicaciones electrónicas, habían sido en realidad escritos por los presuntos terroristas o, en cambio, eran atribuibles a agentes del Estado, que actuaban como agentes provocadores. En este caso, un perito de la fiscalía ofreció testimonio suficiente para convencer al tribunal de la fiabilidad de los métodos y materiales basados en Internet en que se fundaba la acusación, y para asignar el peso correspondiente a la prueba pericial.

396. Cabe señalar que el idioma de estas comunicaciones electrónicas era el árabe y, por tanto, había sido necesario traducirlas al francés, de modo que el fiscal tuvo que presentar al tribunal, junto con la traducción al francés, la transcripción original en árabe. Este aspecto del caso también pone de relieve la atención que se requiere cuando las autoridades tratan de presentar, como prueba, las traducciones de conversaciones y documentos, incluidas las transcripciones de las comunicaciones interceptadas en otros idiomas.

397. Además del testimonio pericial sobre las pruebas digitales, de importancia decisiva, la fiscalía llamó a declarar a peritos en las actividades y objetivos del GIMF; sus métodos de coordinación y reclutamiento de nuevos miembros, de difusión de ideología radical y de instrucción militar; así como los métodos por los cuales se comunicaba a través de Internet. De hecho, la fiscalía presentó informes escritos de dos expertos sobre estos temas, y uno de ellos testificó en juicio para respaldar las conclusiones del informe. El participante del Canadá en la reunión del grupo de expertos hizo hincapié en la importancia de que los fiscales tuvieran más de un testigo pericial en cuestiones probatorias clave, tanto para fines de corroboración como para prevenirse contra imprevistos.

398. Un buen ejemplo del valor de este tipo de pruebas periciales en los juicios en que se formulan cargos relacionados con el apoyo a una organización terrorista es la siguiente declaración del juez de primera instancia, en relación con los “actos reales alentados por el Frente”, que habían sido objeto del testimonio pericial de la acusación:

La defensa invita al Tribunal a concluir que los diferentes mensajes difundidos por el GIMF tenían solo un sentido figurado. El tribunal no tiene ninguna duda al respecto. El contexto de estos mensajes se refiere claramente a actos reales alentados por el Frente. La muerte y destrucción están por todas partes. La yihad que promueve el Frente es de carácter violento. Esta promoción constituye claramente una forma de aliento y, a veces, una amenaza de actividades terroristas. Por tanto, esta actividad encuadra claramente en la definición de actividades terroristas conforme al artículo 83.01 del Código Penal¹⁷².

H. Otras cuestiones

1. Necesidad de prevenirse contra imprevistos y de continuidad

399. La complejidad de los procesamientos relacionados con el terrorismo, en particular los que exigen cooperación internacional o presentan elementos muy técnicos, hacen que sea muy aconsejable contar con un equipo de fiscales para ocuparse de esas causas, y que cada uno de ellos esté familiarizado con los procedimientos y, de ser necesario, en condiciones de continuar la labor en caso de que cualquier miembro del equipo se vea inesperadamente imposibilitado de continuar con la causa. Esta precaución permitirá asegurarse de que los procedimientos se lleven a cabo con un alto nivel de eficiencia y se reduzcan al mínimo las probabilidades de un resultado infructuoso. Los casos de Namouh (Canadá) y Gelowicz, Yilmaz, Schneider y Selek (Alemania) son dos ejemplos útiles de procesamientos complejos y grandes que exigen un enfoque de equipo, con al menos un fiscal en condiciones de participar durante toda la causa. En la de Alemania, cabe observar que la estimación inicial de la duración del juicio había sido de dos años. La duración real fue mucho más corta, debido a las declaraciones de culpabilidad de los acusados, pero aun así el juicio propiamente dicho duró tres meses.

2. *Necesidad de mejorar la formación profesional*

400. Con el fin de asegurar un enfoque integrado de respeto del estado de derecho y de preservación de la integridad de las respuestas de la justicia penal al terrorismo, los países deben contar con procesos sólidos y permanentes para fortalecer la capacidad de los fiscales de aplicar las leyes nacionales contra el terrorismo y cumplir con las obligaciones de cooperación internacional. El carácter de la legislación y de las investigaciones contra el terrorismo, sumado a la velocidad, complejidad y naturaleza transfronteriza de las actividades relacionadas con Internet, significa que los equipos de investigación, incluidos los fiscales, se ven obligados a tomar muchas decisiones relativas a diferentes aspectos del caso, dentro de plazos muy ajustados. Es importante que estén debidamente capacitados y tengan las competencias para desempeñar satisfactoriamente sus funciones básicas en los casos de terrorismo.

401. En los países donde el riesgo de actividades terroristas es alto y la capacidad institucional del ministerio público y otros organismos de justicia penal es baja, debe atribuirse alta prioridad a la formación de especialistas dentro de estos organismos, tanto para el procesamiento de causas penales como para la gestión de los trámites conexos de cooperación internacional.

VII. Cooperación del sector privado

A. Función de los interesados del sector privado

402. Si bien la responsabilidad de la lucha contra el uso de Internet con fines terroristas incumbe, en última instancia, a los Estados Miembros, la cooperación de los principales interesados del sector privado es decisiva para una ejecución eficaz. La infraestructura de las redes de servicios de Internet suele ser propiedad, en su totalidad o en parte, de entidades privadas. Del mismo modo, son empresas privadas, generalmente, las propietarias de las plataformas de medios sociales que facilitan la difusión de contenidos generados por los usuarios a un público más amplio, así como los populares buscadores de Internet, que seleccionan el contenido en función de los criterios proporcionados por el usuario.

403. La eficacia de Internet como medio para la difusión de contenidos relacionados con actos de terrorismo depende de que tanto el autor de la comunicación como su público tengan acceso a las tecnologías de Internet. Por esta razón, los tres métodos principales para limitar el impacto de tales comunicaciones consisten en controlar el acceso a la infraestructura de la red, censurar el contenido de Internet o una combinación de ambos¹⁷³. Si bien el nivel de regulación gubernamental de Internet varía mucho entre los Estados Miembros, a falta de una autoridad mundial y centralizada responsable de la regulación de Internet, los interesados privados, tales como los proveedores de servicios, los sitios web que hospedan contenido generado por los usuarios y los buscadores de Internet siguen desempeñando un importante papel en la regulación de la disponibilidad de contenidos relacionados con el terrorismo difundidos por Internet. La autorregulación por estas partes interesadas del sector privado también puede ayudar en la lucha contra las comunicaciones terroristas y las actividades de incitación, radicalización y adiestramiento llevadas a cabo por medio de Internet. Los servicios privados de monitorización desempeñan asimismo un papel en la detección oportuna de actividades en Internet que pueden promover actos de terrorismo.

1. Proveedores de servicios de Internet

404. En muchos Estados Miembros, el acceso de los usuarios a Internet está controlado por agentes no estatales, como los proveedores privados del sector de telecomunicaciones, que son dueños de la infraestructura de la red o la administran. Estos proveedores de servicios pueden estar en buenas condiciones de ayudar en la reunión de datos sobre

¹⁷³ Conway, "Terrorism and Internet governance: core issues", pág. 26.

las comunicaciones o de revelar estos datos, según proceda¹⁷⁴, facilitando así las investigaciones concretas por la policía, la justicia penal y los servicios de inteligencia de posibles actividades terroristas. Los datos sobre las comunicaciones en poder del proveedor de servicios de Internet pueden constituir pruebas clave contra los autores de delitos relacionados con Internet, o proporcionar enlaces con otras pruebas o colaboradores pertinentes para la investigación.

405. Por ejemplo, los proveedores de servicios de Internet pueden exigir a los usuarios que proporcionen información sobre su identidad antes de darles acceso a los contenidos y servicios de Internet. La reunión y conservación de la información de identificación asociada a los datos de Internet, así como la divulgación de dicha información, con sujeción a las garantías adecuadas, pueden facilitar considerablemente los procedimientos de investigación y enjuiciamiento. En particular, la exigencia de inscribirse para poder usar conexiones inalámbricas con Internet o los servicios de cibercafés podría proporcionar una importante fuente de datos para las investigaciones criminales. Mientras que algunos países, como Egipto, han promulgado legislación que exige al proveedor de servicios de Internet identificar a los usuarios antes de permitirles el acceso a Internet, los propios proveedores de servicios de Internet pueden adoptar medidas similares a título voluntario.

a) Cooperación con las autoridades gubernamentales

406. Teniendo en cuenta lo delicado de los casos relacionados con el terrorismo, las partes interesadas del sector privado pueden sentirse incentivadas a cooperar con las autoridades policiales por el efecto positivo de esa cooperación en su reputación, siempre que la cooperación esté debidamente encuadrada en la necesidad de respetar los derechos humanos fundamentales, como la libertad de expresión, el respeto de la vida privada, el domicilio y la correspondencia, así como el derecho a la protección de los datos personales. El deseo de evitar las consecuencias negativas de la falta de cooperación también podría obrar como aliciente. Por ejemplo, los proveedores de servicios de Internet podrían cooperar por temor a las posibles connotaciones negativas de verse asociados con el apoyo a actividades terroristas. Los problemas de responsabilidad asociados a la acogida de ciertos tipos de contenido de Internet también podrían influir en el nivel de cooperación por parte de las entidades del sector privado.

407. El experto egipcio indicó que la experiencia nacional de Egipto indicaba que las entidades pertinentes del sector privado mostraban una actitud cooperativa cuando recibían solicitudes razonables de las autoridades gubernamentales de restringir el acceso a contenidos relacionados con el terrorismo en Internet. Además, los proveedores de servicios de Internet de Egipto, según se informa, se sienten motivados a colaborar, en parte, por el reconocimiento de la coincidencia de los intereses de los proveedores de servicios de Internet, que podrían ellos mismos ser objeto de ataques terroristas, con los de las autoridades gubernamentales, que procuran prevenir y perseguir esos actos.

408. Si bien las entidades del sector privado pueden sentirse inclinadas a retirar voluntariamente los contenidos ilegales, también pueden estar obligadas a hacerlo por ley. Por ejemplo, en el Reino Unido, el artículo 3 de la Ley de Terrorismo de 2006 prevé notificaciones de retiro, que pueden ser dirigidas a los proveedores de servicios de Internet por las autoridades encargadas de hacer cumplir la ley (véanse los párrafos 172 y ss., *supra*). Las notificaciones de retiro se usan para advertir a los que dan acogida a ciertos contenidos que, a juicio de las autoridades policiales, dicho material está relacionado con el terrorismo y es ilegal. Los proveedores de servicios de Internet que reciben una notificación de retiro están obligados a eliminar el contenido relacionado con el terrorismo dentro de los dos días hábiles. Si bien hay jurisdicciones que también emplean notificaciones de retiro para otros delitos, lo más común es que se trate de casos de infracción de derechos de autor o de contenido sexualmente explícito.

409. El Estado de Israel destacó sus logros en relación con la cooperación de los representantes del sector privado extranjero en Israel. Por ejemplo, en varias investigaciones de delitos informáticos, se hicieron solicitudes a los representantes de Microsoft y Google en Israel. Tras la recepción de una orden judicial debidamente notificada, se proporcionó de inmediato la información solicitada por las autoridades investigadoras. En algunos casos en que había sido necesario dirigir las solicitudes a representantes del sector privado con sede en los Estados Unidos, se empleó, en la mayoría de los casos, el procedimiento oficial de solicitar asistencia judicial por conducto de las autoridades gubernamentales, salvo algunos casos aislados en que se recurrió con éxito a las solicitudes directas de datos de identificación a las empresas extranjeras del sector privado.

b) Retención de los datos

410. Varios Estados Miembros han introducido recientemente, o se proponen introducir, legislación por la cual se exige a los proveedores de servicios de telecomunicaciones que capturen y archiven de forma automática los datos de las comunicaciones de sus usuarios. En 2006, impulsada en parte por los ataques terroristas de Madrid en 2004 y Londres en 2005¹⁷⁵, la Unión Europea aprobó una directiva sobre la retención obligatoria de los datos de tráfico de las comunicaciones (Directiva 2006/24/CE del Parlamento Europeo y del Consejo de la Unión Europea, 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)¹⁷⁶. La Directiva 2006/24/CE reconoce las dificultades causadas por las diferencias legales y técnicas entre las disposiciones nacionales relativas a los tipos de datos que deben retenerse, así como en cuanto a las condiciones y los períodos de retención de los datos¹⁷⁷. Por tanto, la Directiva tiene por objeto armonizar las obligaciones mínimas de retención de datos

¹⁷⁵ Comisión Europea, "Informe de la Comisión al Consejo y al Parlamento Europeo: Informe de evaluación sobre la Directiva de conservación de datos (Directiva 2006/24/CE)", documento COM(2011) 225 (Bruselas, 18 de abril de 2011), secc. 3.2.

¹⁷⁶ *Diario Oficial de la Unión Europea*, L 105, 13 de abril de 2006.

¹⁷⁷ *Ibid.*, preámbulo, párr. 6.

de los proveedores de servicios de comunicaciones electrónicas que operan en los Estados miembros de la Unión Europea para fines de prevención, investigación, detección y enjuiciamiento de delitos.

411. La Directiva 2006/24/CE obliga a los Estados miembros a adoptar legislación¹⁷⁸ que exija a los proveedores de telecomunicaciones retener determinados datos de tráfico relativos a las comunicaciones electrónicas¹⁷⁹ durante un período de entre seis meses y dos años. Estos datos de tráfico incluyen la información necesaria para identificar al iniciador y al destinatario del correo y de las comunicaciones de telefonía de Internet, junto con información sobre la hora, la fecha y la duración de las comunicaciones electrónicas, pero no se extiende a su contenido¹⁸⁰. Estos datos deben ponerse a disposición, en relación con la investigación, la detección y el enjuiciamiento de delitos graves, de las autoridades policiales nacionales y, por conducto de las autoridades nacionales¹⁸¹, de sus homólogos de otros Estados miembros de la Unión Europea, de acuerdo con los requisitos de la legislación nacional respectiva.

412. Por ejemplo, una vez incorporados estos principios a la legislación nacional y con sujeción a los requisitos de procedimiento, las autoridades nacionales de aplicación de la ley pueden solicitar el acceso a los datos en poder de los proveedores de servicios para identificar a los abonados que utilizan una dirección IP específica y a aquellos con quienes esas personas han estado en contacto durante un período de tiempo determinado¹⁸². Además, las investigaciones de los actos terroristas pueden basarse en los datos retenidos por los proveedores de servicios, lo cual refleja el tiempo necesario para planificar el acto y permite detectar las pautas de comportamiento delictivo y las relaciones entre los cómplices del acto, y establecer la intención dolosa¹⁸³. Algunos Estados miembros de la Unión Europea¹⁸⁴ han indicado que los registros de retención de datos son el único medio de investigar ciertos delitos que entrañan la comunicación por Internet, tales como los anuncios en salas de charla, que pueden rastrearse solo a través de los datos de tráfico de Internet¹⁸⁵. Varios Estados miembros de la Unión Europea¹⁸⁶ también han informado del uso de datos retenidos por los proveedores de servicios para exculpar a personas de quienes se sospechaba la comisión de delitos sin tener que recurrir a otros métodos de vigilancia más intrusivos, tales como la interceptación y los registros domiciliarios. Los datos sobre la ubicación física también son importantes cuando la policía los emplea para excluir a sospechosos del lugar de los hechos y para verificar coartadas. Los datos retenidos con arreglo a la legislación promulgada también

¹⁷⁸En abril de 2011, había leyes en vigor de este tipo en 22 Estados miembros de la Unión Europea.

¹⁷⁹Esto incluye los datos generados o tratados por los proveedores de servicios en el curso de sus actividades, como por ejemplo, la transmisión de una comunicación, facturación, interconexión, pagos, comercialización y otros servicios de valor agregado.

¹⁸⁰*Diario Oficial de la Unión Europea*, L 105, 13 de abril de 2006, art. 5.

¹⁸¹*Ibid.*, art. 4.

¹⁸²Comisión Europea, “Informe de la Comisión al Consejo y al Parlamento Europeo: Informe de evaluación sobre la Directiva de conservación de datos (Directiva 2006/24/CE)”, secc. 5.2.

¹⁸³*Ibid.*, secciones 3.1 y 5.2.

¹⁸⁴Bélgica, Irlanda y el Reino Unido.

¹⁸⁵Comisión Europea, “Informe de la Comisión al Consejo y al Parlamento Europeo: Informe de evaluación sobre la Directiva de conservación de datos (Directiva 2006/24/CE)”, secc. 5.4.

¹⁸⁶Alemania, Eslovenia, Polonia y el Reino Unido.

permiten reconstruir las pistas de elementos de prueba que llevan a un acto de terrorismo, incluso al facilitar el establecimiento o la corroboración de otras formas de pruebas sobre las actividades y los vínculos entre distintos sospechosos¹⁸⁷.

2. *Sitios web y otras plataformas que hospedan contenido generado por los usuarios*

413. Los contenidos relacionados con el terrorismo hospedados en sitios web populares que presentan material generado por el usuario tienen la posibilidad de llegar a un público mucho más amplio que el contenido de los sitios web tradicionales, tableros de anuncios y foros web especializados, que generalmente atraen a un grupo de personas autoseleccionado. Según el sitio web de intercambio de videos YouTube, cada minuto los usuarios suben a ese sitio 48 horas de videos generados por usuarios, lo que equivale a casi ocho años de contenido cargado por día¹⁸⁸. El hecho de poder llegar, según se estima, a ocho millones de usuarios de YouTube al mes, usuarios únicos por sus características, reduce considerablemente las barreras para el acceso a contenidos relacionados con el terrorismo. El fuerte aumento de la popularidad de los contenidos generados por usuarios en los últimos años acrecienta la dificultad logística de monitorizar los contenidos relacionados con el terrorismo. Además, los usuarios de los sitios web de hospedaje de videos pueden encontrarse, sin querer, con contenido relacionado con el terrorismo, como resultado de la búsqueda o la visualización de material más moderado, debido a los mecanismos integrados que sugieren automáticamente contenidos semejantes.

La causa Filiz G.

En esta causa alemana, la acusada, Filiz G., fue declarada culpable de los cargos de reclutamiento de miembros o simpatizantes de organizaciones terroristas extranjeras (Al-Qaida, la Unión de la Yihad Islámica y los Deutsche Taliban Mujahideen) y de prestar apoyo a esas organizaciones.

En marzo de 2009, la acusada se unió a un foro de Internet y comenzó a publicar traducciones al alemán de comunicados de organizaciones terroristas que denunciaban presuntos delitos de las fuerzas armadas internacionales en el Iraq y el Afganistán, y pedían a los usuarios que se unieran a la yihad o la apoyaran. Filiz G., que era la esposa de un terrorista alemán preso, no tardó en adquirir derechos de administración del foro de Internet. En el momento de su detención, en febrero de 2010, la acusada había publicado más de 1.000 anuncios y comentarios, tanto en una parte de acceso público del foro de Internet como en una sección privada, accesible solo para los usuarios registrados. Filiz G. abrió nueve canales de video en el portal de YouTube, y cargó en todos ellos 101 videos, que incluían tanto los filmados por grupos terroristas, como Al-Qaida y la Unión de la Yihad Islámica,

¹⁸⁷ Comisión Europea, “Informe de la Comisión al Consejo y al Parlamento Europeo: Informe de evaluación sobre la Directiva de conservación de datos (Directiva 2006/24/CE)”, secc. 5.4.

¹⁸⁸ Las estadísticas de YouTube pueden consultarse en www.youtube.com/t/press_statistics.

como videos que ella misma había producido. La acusada había colaborado muy estrechamente con M., el “coordinador de los medios de comunicación” de la Unión de la Yihad Islámica. M. se había comunicado con ella por Internet y en un principio le pidió que tradujera textos con contenido religioso del turco al alemán. Posteriormente, le dio los enlaces a los videos, que la acusada publicó en YouTube, y le pidió que ayudara con la obtención de donaciones.

- En un caso, la acusada tradujo al alemán un artículo publicado en una página web en lengua turca y lo publicó en una página web alemana. El artículo hacía un llamamiento a los donantes para que apoyaran a “las familias de los muyahidines del Afganistán, que están resistiendo los crueles ataques de las naciones de cruzados”. El texto iba acompañado de siete fotos; una mostraba diferentes alimentos y las otras seis eran de niños armados con rifles de asalto y otras armas.

Además de la publicación de artículos para la recaudación de fondos, la acusada también estuvo implicada en la percepción efectiva de fondos. Para preservar el anonimato de los donantes, abrió un apartado de correos, al que los donantes dirigían sobres con su nombre de usuario de Internet que contenían dinero en efectivo (en general, las contribuciones eran de unos cuantos cientos de euros). A continuación, utilizó los servicios financieros de Western Union para transferir los fondos a un intermediario en Turquía, que los envió, a su vez, a M., en Waziristán. La acusada también publicó videos en Internet en los que agradecía a los donantes (a quienes asignó, para este fin, apodos relacionados con sus nombres de usuario de Internet) y los informaba de la marcha de la campaña de recaudación de fondos.

En el juicio, en marzo de 2011, la acusada admitió los cargos y fue condenada a dos años y medio de prisión. Al sentenciarla, el tribunal consideró que la acusada había sido plenamente consciente de que el material de propaganda que difundía procedía de organizaciones terroristas y de que los fondos que había recaudado y transferido estaban destinados a comprar, además de bienes humanitarios, armas y municiones para esas organizaciones. Observando que los delitos se habían cometido principalmente a través de Internet, el juez de sentencia declaró:

[...] el tribunal atribuye particular importancia a la gran peligrosidad de la difusión de propaganda yihadista por Internet. Los materiales, una vez subidos a Internet, ya no pueden, prácticamente, ser controlados ni eliminados de la web, ya que los demás usuarios pueden descargarlos, utilizarlos y darles mayor difusión. Dado el alcance casi mundial de este medio y el número de usuarios inmensamente alto y en continuo aumento, Internet constituye una plataforma de importancia cada vez mayor para los grupos terroristas, que difunden desde ella sus objetivos y su propaganda, y crean en todo el mundo un clima de temor a una amenaza terrorista omnipresente. La difusión de material como el publicado por la acusada equivale a un “incendio intelectual deliberado”. Es incomparablemente más duradera en sus efectos y por tanto más peligrosa que, por ejemplo, la difusión de propaganda mediante folletos u otros medios de comunicación impresos.

414. La causa del Reino Unido *R. c. Roshanara Choudhry* es un buen ejemplo de una persona autodidacta, la Sra. Choudhry, que se radicalizó, hasta el punto de cometer un acto violento, exclusivamente a causa de material accesible por Internet y, en particular, por medio de sitios web de videos. El caso de la Sra. Choudhry atrajo atención internacional por la facilidad con que una plataforma de intercambio de videos, que presentaba contenido generado por los usuarios, le había permitido localizar y ver videos

de contenido extremista islámico, y por el proceso que la había llevado a tomar la decisión de cometer un acto de terrorismo después de ver sistemáticamente estos contenidos a lo largo de varios meses.

415. En 2010, a raíz de conversaciones con los Gobiernos del Reino Unido, iniciadas por la unidad especializada en derivaciones, en la lucha contra el uso de Internet por terroristas, y los Estados Unidos, donde se encuentran los servidores de YouTube, la compañía matriz de YouTube, Google Inc., implantó voluntariamente un sistema que permite a los usuarios alertar sobre contenidos posiblemente relacionados con el terrorismo en el sitio web de YouTube. Este mecanismo representa una importante herramienta para la identificación proactiva de contenidos que pueden promover actos de terrorismo.

416. Algunos sitios web y plataformas de medios sociales también incluyen disposiciones en sus condiciones de uso que prohíben el uso de sus servicios para promover, entre otras cosas, las actividades terroristas. Por ejemplo, las condiciones de servicio de Twitter¹⁸⁹, red de información en tiempo real, prohíbe el uso del servicio para la publicación de amenazas directas y específicas de violencia contra terceros o para cualquier propósito ilegal o en apoyo de actividades ilícitas¹⁹⁰. En caso de incumplimiento de dichas condiciones, el proveedor de servicios se reserva el derecho (aunque no está obligado a hacerlo) de eliminar o rechazar la distribución de contenido ofensivo o interrumpir el servicio. Además, no pueden ser usuarios de Twitter los que tengan prohibido recibir servicios con arreglo a las leyes de los Estados Unidos o cualquier otra jurisdicción aplicable, lo que excluye el uso de sus servicios por parte de organizaciones designadas como terroristas. Sin embargo, aun cuando existan esas condiciones, pueden surgir dificultades en la aplicación, debido en parte a la amplia base de usuarios y el alto volumen resultante de contenido generado por usuarios que hay que monitorizar.

417. Noticias recientes indican que, en el caso de infracción de los derechos de autor, Google suele intervenir para eliminar contenidos o enlaces ilegales dentro de las seis horas de haber recibido una solicitud en ese sentido, a pesar de haber estado inundados con más de cinco millones de solicitudes de ese tipo en 2011¹⁹¹. La combinación de un mecanismo de alerta sobre el contenido y una respuesta igualmente diligente y oportuna en cuanto a contenidos presuntamente relacionados con el terrorismo sería un progreso muy positivo en la lucha contra el uso de Internet para el reclutamiento, la radicalización, el adiestramiento y la glorificación de los actos de terrorismo y la incitación a cometerlos.

418. El contenido difundido por las organizaciones terroristas suele estar identificado con designaciones características que, según se sabe, están asociadas con organizaciones

¹⁸⁹Pueden consultarse en <https://twitter.com/tos>.

¹⁹⁰Véase <http://support.twitter.com/articles/18311-the-twitter-rules#>.

¹⁹¹Jenna Wortham, "A political coming of age for the tech industry", *The New York Times*, 17 de enero de 2012. Puede consultarse en www.nytimes.com/2012/01/18/technology/web-wide-protest-over-two-antipiracy-bills.html?hp.

particulares¹⁹². La monitorización y eliminación de dicho contenido fácilmente identificable por los sitios web que lo hospedan puede ofrecer beneficios considerables en la lucha contra la difusión de propaganda terrorista ilegal. Además, el uso de mecanismos de alerta, similares a los introducidos en YouTube, como característica estándar de otros medios de comunicación de redes sociales y buscadores de Internet, puede aumentar la probabilidad de eliminación oportuna de propaganda destinada a promover el terrorismo. La intensificación de las medidas para detectar los contenidos relacionados con el terrorismo, combinada con arreglos mejorados, oficiales y oficiosos, de intercambio de información entre el Estado y los agentes privados, podría ayudar apreciablemente a detectar y combatir las actividades terroristas que usan Internet.

419. El intercambio de información es particularmente importante en el contexto de la distinción entre el contenido en línea que puede ser objetable y el que puede ser ilegal (véase la discusión en la sección I.B.1). Por ejemplo, si bien el sistema de alerta utilizado por YouTube puede ayudar a priorizar determinados contenidos para su examen, a continuación deberá determinarse si dicho contenido transpone el umbral prescrito para ser retirado o bloqueado. El diálogo oficioso entre el proveedor de servicios de Internet o los sitios web, por un lado, y los funcionarios de la justicia penal, por el otro, puede facilitar este proceso. Para ello, puede alentarse a las entidades pertinentes del sector privado a cooperar con las autoridades policiales denunciando los contenidos objetables que susciten sospechas de tener conexiones con cualquier usuario afiliado a una organización terrorista conocida o de promover las actividades de dicha organización.

3. *Buscadores de Internet*

420. Los buscadores de Internet proporcionan un puente entre los contenidos de Internet y el usuario final. El contenido excluido de estos buscadores tiene un público mucho más reducido. Algunos buscadores de Internet, como Google y Yahoo, censuran voluntariamente el contenido que consideran delicado o perjudicial para sus intereses. Por ejemplo, después de los atentados del 11 de septiembre de 2001 en los Estados Unidos, muchos buscadores de Internet eliminaron los resultados de búsquedas relacionados con posibles organizaciones terroristas¹⁹³. Los funcionarios responsables de la formulación de políticas y los encargados de hacer cumplir la ley de varios Estados Miembros han fomentado las iniciativas similares a título voluntario para reducir la facilidad de acceso a través de los buscadores de Internet a contenidos que pueden promover actos violentos. También podría ser beneficiosa la aplicación voluntaria por los buscadores de un sistema de alerta sobre contenidos relacionados con el terrorismo, de manera similar al introducido por YouTube.

¹⁹²“Jihadist use of social media: how to prevent terrorism and preserve innovation”, testimonio de A. Aaron Weisburd, Director, Society for Internet Research, ante el Subcomité de Lucha contra el Terrorismo y de Inteligencia, Comité de Seguridad Interior, de la Cámara de Representantes de los Estados Unidos, 6 de diciembre de 2011.

¹⁹³Conway, “Terrorism and Internet governance: core issues”, pág. 30.

4. Servicios de monitorización

421. Algunas entidades privadas han adoptado un enfoque más estructurado de la lucha contra las actividades terroristas en Internet. Los servicios de monitorización, tales como Search for International Terrorist Entities (SITE) (Búsqueda de Entidades Terroristas Internacionales), con sede en los Estados Unidos, e Internet Haganah monitorizan y reúnen información de código abierto relacionada con organizaciones terroristas¹⁹⁴. SITE, que funciona como un servicio de inteligencia, obtiene importantes ingresos derivados de suscripciones. En tales condiciones, SITE y otras organizaciones similares pueden, por tanto, tener mayor acceso a los recursos necesarios para permitir la rápida detección y traducción, en su caso, de las actividades en Internet que pueden promover actos de terrorismo. Internet Haganah, en cambio, monitoriza las actividades en Internet de grupos extremistas islámicos con el fin de detectar y bloquear el acceso a los contenidos relacionados con el terrorismo. Internet Haganah se financia en parte mediante donaciones y funciona fundamentalmente sobre la base de las aportaciones de una red de voluntarios. Este servicio de monitorización investiga y detecta de manera proactiva los contenidos de Internet que considera relacionados con el terrorismo y el correspondiente sitio web que los hospeda. Esta información puede ser compartida con las autoridades policiales o el público o ser utilizada para comunicarse con el sitio web a fin de conseguir la eliminación de los contenidos o el bloqueo del acceso¹⁹⁵. Mientras que los modelos de uso y funcionamiento de estos servicios de monitorización son diferentes, ambos promueven la rápida detección de los contenidos relacionados con el terrorismo en Internet, lo cual puede ser útil para la reunión de inteligencia, la investigación y el enjuiciamiento de tales actividades.

B. Asociaciones entre el sector público y el privado

422. El establecimiento de asociaciones entre las partes interesadas de los sectores público y privado en la lucha contra el uso de Internet con fines terroristas puede reportar muchos beneficios. Las dificultades que suelen mencionarse en cuanto a la cooperación de los sectores público y privado en relación con la ciberdelincuencia en general son la falta de comunicación entre las autoridades policiales y los proveedores de servicios en relación con la reunión eficiente de las pruebas, y el conflicto entre los requisitos de la privacidad y la necesidad de retención de los datos para las posibles actuaciones judiciales. La creación de un foro para el diálogo formal e informal entre los homólogos de los sectores público y privado podría mitigar considerablemente tales preocupaciones. Además de las oportunidades que ofrecería mediante la celebración de reuniones periódicas entre los asociados, la organización de actividades tales como la ejecución de programas conjuntos de formación también podría ayudar a superar las barreras de comunicación y fomentar la confianza entre los miembros de la asociación¹⁹⁶.

¹⁹⁴Ibid, pág. 31.

¹⁹⁵Ariana Eunjung Cha, "Watchdogs seek out the web's bad side", *Washington Post*, 25 de abril de 2005. Puede consultarse en www.washingtonpost.com/wp-dyn/content/article/2005/04/24/AR2005042401473.html.

¹⁹⁶Instituto Interregional de las Naciones Unidas para Investigaciones sobre la Delincuencia y la Justicia, "Public-private partnerships for the protection of vulnerable targets against terrorist attacks: review of activities and findings" (enero de 2009), párr. 23.

423. Se ha avanzado mucho en el establecimiento de asociaciones entre el sector público y el privado en asuntos de seguridad relacionados con posibles ataques terroristas contra objetivos vulnerables o la infraestructura, o en relación con la prevención y persecución de la ciberdelincuencia en general. El establecimiento de asociaciones similares entre los sectores público y privado en relación con la regulación del uso de Internet con fines terroristas sería beneficioso. Un buen ejemplo de una fructífera asociación de esos sectores relacionada con la seguridad es el Overseas Security Advisory Council, establecido entre el Departamento de Estado de los Estados Unidos de América y organizaciones norteamericanas del sector privado que operan en el extranjero. El Consejo ofrece un foro para el intercambio de las mejores prácticas y una plataforma para el intercambio periódico y oportuno de información entre el sector privado y el Gobierno de los Estados Unidos sobre la evolución del entorno de seguridad en el extranjero, en particular en relación con el terrorismo, así como sobre los factores políticos, económicos y sociales que pueden incidir en el entorno de seguridad a nivel mundial y en cada país¹⁹⁷.

424. El Equipo de Respuesta a Incidentes de Seguridad en la Infraestructura de Internet, de Indonesia, es otro ejemplo de una iniciativa de seguridad centrada en la asociación de los sectores público y privado. Reúne a representantes de los servicios de correos y telecomunicaciones, la Policía Nacional, la Fiscalía General de la Nación, el Banco de Indonesia, la Asociación Indonesia de Proveedores de Servicios de Internet, la Asociación Indonesia de Cibercafés, la Asociación Indonesia de Tarjetas de Crédito y la Sociedad Indonesia TIC (MASTEL). Los miembros cooperan, entre otras cosas, en las actividades de monitorización, detección y alerta temprana de amenazas e interrupciones en las redes de telecomunicaciones basadas en protocolos de Internet; tareas de investigación y desarrollo; establecimiento de laboratorios de simulación y capacitación en la seguridad del uso de las telecomunicaciones basadas en protocolos de Internet; prestación de servicios de consultoría y asistencia técnica a las entidades o instituciones estratégicas. El Equipo de Respuesta servirá como centro de coordinación de las entidades o instituciones pertinentes, nacionales e internacionales¹⁹⁸.

425. En noviembre de 2006 se reunió en Moscú el Foro mundial sobre la asociación entre los Estados y el sector empresarial en la lucha contra el terrorismo. Como resultado de esta reunión, el Grupo de los Ocho¹⁹⁹ adoptó la Estrategia de Asociación entre el Estado y el sector empresarial en la lucha contra el terrorismo²⁰⁰, que promueve, entre otras cosas, la cooperación entre los proveedores de servicios de Internet y otras empresas y las autoridades gubernamentales para contrarrestar el uso indebido de Internet por los terroristas y prevenir la facilitación de los últimos pasos que conducen del extremismo al terrorismo. De acuerdo con esta estrategia, se alienta a los gobiernos a crear asociaciones nacionales e internacionales voluntarias más estrechas con los proveedores de servicios de Internet a fin de combatir el uso de Internet en actividades

¹⁹⁷Ibid., párr. 9.

¹⁹⁸Comunicación escrita del experto de Indonesia.

¹⁹⁹Foro oficioso de los Jefes de Estado de los siguientes países industrializados: Alemania, Canadá, Estados Unidos, Federación de Rusia, Francia, Italia, Japón y Reino Unido.

²⁰⁰A/61/606-S/2006/936, anexo.

tales como el reclutamiento, el adiestramiento y la incitación a cometer actos terroristas.

426. Otras iniciativas pertinentes de colaboración entre el sector público y el privado incluyen la creación en 2007 del Grupo de Trabajo del Consejo de Europa, con participantes de las fuerzas del orden, la empresa y las asociaciones de proveedores de servicios, para abordar las cuestiones relacionadas con la ciberdelincuencia en general. Esta iniciativa tiene por objeto estrechar la cooperación entre las autoridades policiales y el sector privado, con el fin de hacer frente a la ciberdelincuencia de manera más eficiente.

427. En 2010, la Comisión Europea aprobó y financió un proyecto que entrañaba la colaboración entre el mundo académico, la empresa y la policía y tenía por objeto crear una red de Centros de Excelencia para la Formación, Investigación y Educación en materia de Ciberdelincuencia (2CENTRE) en Europa. Esa red actualmente ofrece capacitación en centros nacionales de excelencia ubicados en Irlanda y Francia. Cada centro nacional se basa en una alianza entre los representantes de la fuerza pública, la empresa y el mundo académico, que colaboran para desarrollar los programas de formación y las herramientas pertinentes para su uso en la lucha contra la ciberdelincuencia (véase la sección IV.G).

428. Las asociaciones entre el sector público y el privado dirigidas específicamente contra el uso de Internet por terroristas también podrían proporcionar un medio para promover directrices claras sobre el intercambio de información entre el sector privado y el público, de conformidad con las normas aplicables de protección de datos. Las “Directrices para la cooperación entre las autoridades responsables de velar por el cumplimiento de la ley y los proveedores de servicios de Internet en la lucha contra la ciberdelincuencia”²⁰¹, del Consejo de Europa, proporcionan una buena base para orientar el intercambio de información. El objetivo de estas directrices es el establecimiento de relaciones de confianza mutua y de cooperación entre las partes interesadas del sector público y el privado como base para la cooperación. Las directrices también hacen hincapié en la necesidad de promover procedimientos de cooperación eficaces y rentables. Se alienta a las fuerzas del orden y a los proveedores de servicios de Internet a participar en el intercambio de información a fin de fortalecer su capacidad para detectar y combatir la ciberdelincuencia mediante la celebración de reuniones periódicas y el intercambio de buenas prácticas y datos sobre los resultados. Las directrices también alientan el establecimiento de asociaciones oficiales y procedimientos escritos, como base de relaciones a más largo plazo, a fin de garantizar, entre otras cosas, que haya protecciones adecuadas de que la asociación no infrinja los derechos de los participantes del sector privado ni las facultades legales de las fuerzas del orden²⁰².

²⁰¹ Consejo de Europa, División de Delitos Económicos, “Directrices para la cooperación entre las autoridades responsables de velar por el cumplimiento de la ley y los proveedores de servicios de Internet en la lucha contra la ciberdelincuencia” (Estrasburgo, 2 de abril de 2008). Puede consultarse en http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/lea_isp/567_prov-d-guidelines_provisional2%20_3%20April%202008_final_spanish.pdf.

²⁰² *Ibid.*, párrs. 10 a 13.

429. A continuación figuran algunas de las medidas recomendadas para ser adoptadas por las fuerzas del orden de conformidad con las directrices:

- Participar en una amplia cooperación estratégica con los proveedores de servicios de Internet, incluso realizando periódicamente seminarios de capacitación técnica y jurídica, y proporcionar información sobre los resultados de las investigaciones realizadas o la inteligencia reunida, a partir de informes o denuncias procedentes de los proveedores de servicios de Internet
- Ofrecer explicaciones y asistencia a los proveedores de servicios de Internet en relación con las técnicas de investigación que no estén directamente relacionadas con un caso entre manos, a fin de facilitar la comprensión de las razones por las cuales la cooperación de los proveedores de servicios de Internet da lugar a investigaciones más eficientes
- Otorgar prioridad a las solicitudes de grandes volúmenes de datos, evitando costos innecesarios y el entorpecimiento de las operaciones comerciales²⁰³.

430. A continuación figuran algunas de las medidas recomendadas para su adopción por los proveedores de servicios de Internet de acuerdo con las directrices:

- Cooperar para reducir al mínimo el uso de los servicios con fines ilícitos
- Notificar las actividades delictivas a las fuerzas del orden
- Siempre que sea posible, proporcionar una lista, previa solicitud, de los tipos de datos correspondientes a cada servicio que podrían facilitarse a las fuerzas del orden tras recibir una solicitud válida de divulgación²⁰⁴.

431. Las asociaciones entre el sector público y el privado pueden proporcionar también un foro a fin de promover normas mínimas para la retención segura de los datos por las partes interesadas del sector privado y de mejorar los canales de comunicación para la transmisión de información por las partes interesadas del sector privado respecto de las actividades sospechosas.

²⁰³Ibid., párrs. 17, 29, 30 y 33.

²⁰⁴Ibid., párrs. 41, 42 y 50.

VIII. Conclusiones

A. Uso de Internet con fines terroristas

432. En los primeros capítulos del presente documento se proporciona una vista panorámica, desarrollada a lo largo de líneas funcionales, de los medios por los que Internet suele usarse para promover y apoyar actos de terrorismo, en particular en la forma de propaganda (incluida la que persigue fines de reclutamiento, radicalización e incitación al terrorismo), adiestramiento y financiación, y de planificación y ejecución de dichos actos. También se hace hincapié en las oportunidades que ofrece Internet para prevenir, detectar y frustrar los actos de terrorismo. Estas pueden incluir actividades de reunión de inteligencia y de otro tipo para prevenir y combatir los actos de terrorismo, así como la obtención de pruebas para el enjuiciamiento de esos actos.

433. Los contraargumentos y otras comunicaciones estratégicas pueden ser un medio eficaz de desbaratar el proceso de radicalización e inculcación de ideales extremistas, que a su vez pueden manifestarse en actos de terrorismo. También es importante una comprensión cabal de las cuestiones más generales que sustentan la radicalización a fin de entablar un diálogo constructivo con reclutas potenciales para la causa terrorista, y de promover medios alternativos legales de perseguir aspiraciones políticas, sociales o religiosas legítimas.

434. El respeto por los derechos humanos y el estado de derecho es parte integrante de la lucha contra el terrorismo. En particular, los Estados Miembros reafirmaron esas obligaciones en la Estrategia global de las Naciones Unidas contra el terrorismo, “reconociendo que las medidas eficaces contra el terrorismo y la protección de los derechos humanos no son objetivos contrapuestos, sino que se complementan y refuerzan mutuamente”. La aplicación efectiva del enfoque del estado de derecho para luchar contra el uso de Internet con fines terroristas debe ser objeto de una evaluación constante, durante todas las etapas de las iniciativas de lucha contra el terrorismo, desde la reunión de inteligencia preventiva hasta la observancia de las garantías procesales en el enjuiciamiento de los sospechosos.

B. Contexto internacional

435. Actualmente no hay ningún tratado amplio de las Naciones Unidas contra el terrorismo, ni tampoco existe una definición oficial del término “terrorismo”. Sin embargo, los Estados Miembros de las Naciones Unidas se encuentran en vías de redactar un convenio general sobre el terrorismo internacional, que complementará el actual marco jurídico internacional relativo a la lucha contra el terrorismo. Este marco

consiste en una variedad de fuentes, incluidas las resoluciones de la Asamblea General y del Consejo de Seguridad, los tratados, la jurisprudencia y el derecho internacional consuetudinario. Varios instrumentos regionales y subregionales también ofrecen valiosas normas de fondo y de procedimiento para penalizar los actos de terrorismo que pueden cometerse por medio de Internet.

436. Los Estados Miembros han resuelto, en cumplimiento de la Estrategia global de las Naciones Unidas contra el terrorismo, adoptar medidas urgentes para prevenir y combatir el terrorismo en todas sus formas y manifestaciones y, en particular:

- a) Considerar la posibilidad de pasar a ser partes sin demora en los convenios y protocolos internacionales existentes de lucha contra el terrorismo y de aplicarlos, y hacer todo lo posible para llegar a un acuerdo sobre un convenio general sobre el terrorismo internacional y concertarlo;
- b) Aplicar todas las resoluciones de la Asamblea General sobre medidas para eliminar el terrorismo internacional, así como las resoluciones pertinentes de la Asamblea sobre la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo;
- c) Aplicar todas las resoluciones del Consejo de Seguridad relacionadas con el terrorismo internacional y cooperar plenamente con los órganos subsidiarios del Consejo de Seguridad dedicados a la lucha contra el terrorismo en la realización de sus tareas.

C. Marcos normativo y legislativo

I. Marco normativo

437. Una respuesta eficaz de la justicia penal a las amenazas que plantea el uso de Internet por los terroristas exige que los gobiernos establezcan políticas y leyes nacionales claras que se ocupen, entre otras cosas, de: *a)* la penalización de los actos ilícitos cometidos por terroristas a través de Internet o servicios conexos; *b)* el otorgamiento de facultades especiales de investigación a los organismos de seguridad encargados de las investigaciones relacionadas con el terrorismo; *c)* la regulación de los servicios relacionados con Internet (por ejemplo, los proveedores de servicios de Internet) y el control del contenido; *d)* la facilitación de la cooperación internacional; *e)* el desarrollo de procedimientos especializados judiciales o probatorios; y *f)* la observancia de las normas internacionales de derechos humanos.

438. La clasificación general de los enfoques estratégicos proporcionados por el Grupo de Trabajo sobre medidas para hacer frente al uso de Internet con fines terroristas, del Equipo Especial sobre la Ejecución de la Lucha contra el Terrorismo, que comprende el uso de la legislación general sobre ciberdelincuencia, la legislación antiterrorista general (no específicamente relacionada con Internet) y la legislación antiterrorista específicamente relacionada con Internet, constituye un marco conceptual útil para los

encargados de formular políticas y los legisladores. En la actualidad, son pocos los Estados que han elaborado leyes dirigidas específicamente contra los actos cometidos por terroristas a través de Internet. La mayoría de los países invocan las leyes penales generales, sobre ciberdelincuencia o contra el terrorismo, o todas ellas, para penalizar este tipo de delitos y enjuiciar a los autores.

2. Marco legislativo

439. Además de servirse de Internet como parte de las actividades para perpetrar delitos graves (por ejemplo, atentados con bombas), los terroristas pueden recurrir a Internet para llevar a cabo otras actividades de apoyo (por ejemplo, difusión de propaganda o reclutamiento y adiestramiento de los miembros). Los países han adoptado diferentes enfoques para penalizar los actos ilícitos de terrorismo cometidos a través de Internet.

440. En su resolución 1624 (2005), el Consejo de Seguridad, entre otras cosas, instó a los Estados a penalizar la incitación a la comisión de actos de terrorismo. Los Estados están obligados, en virtud de la resolución y otros instrumentos internacionales, a velar por que las medidas destinadas a combatir los actos de incitación al terrorismo estén en plena conformidad con sus obligaciones internacionales en virtud de la legislación sobre derechos humanos, el derecho de los refugiados y el derecho humanitario.

441. La necesidad de proteger plenamente los derechos humanos (por ejemplo, el derecho a la libertad de expresión) al tiempo que se elaboran y aplican las leyes que penalizan la incitación a cometer actos de terrorismo presenta un desafío permanente a los responsables de formular políticas, los legisladores, las fuerzas del orden y los fiscales de todos los países. Los Estados han adoptado diferentes enfoques para penalizar los actos de incitación al terrorismo. Algunos países han tipificado específicamente los actos de incitación o glorificación del terrorismo, mientras que otros se basan en los actos delictivos preparatorios como la instigación o la asociación ilícita.

442. La investigación de los casos de terrorismo en que los presuntos terroristas han usado Internet u otros servicios conexos suele exigir el uso de tipos especializados de facultades de investigación por los organismos encargados de hacer cumplir la ley. La mayoría de los gobiernos han promulgado leyes que permiten a las fuerzas del orden llevar a cabo actividades de este tipo en las investigaciones relacionadas con el terrorismo. Estas técnicas de investigación deben estar debidamente autorizadas por las leyes nacionales y emplearse de manera que se respeten los derechos humanos fundamentales protegidos por las normas internacionales de derechos humanos.

443. Las autoridades necesitan la cooperación de los operadores de telecomunicaciones cuando recurren a la monitorización electrónica, las escuchas telefónicas y técnicas similares de investigación electrónica. Es aconsejable que los gobiernos proporcionen una base jurídica clara para las obligaciones de las partes del sector privado, incluidas las especificaciones técnicas requeridas de sus redes y cómo han de sufragarse los gastos de dotarlas de esa capacidad.

444. Se sabe que los terroristas han utilizado cibercafés para llevar a cabo sus actividades; sin embargo, no se sabe hasta qué punto esto constituye un problema. Algunos gobiernos han impuesto obligaciones específicas a los operadores de los cibercafés, a efectos del cumplimiento de la ley (incluida la lucha contra el terrorismo), de obtener, conservar y, previa solicitud, presentar a las fuerzas del orden identificación fotográfica, domicilio y datos de uso y conexión de los clientes. Cabe cuestionar la utilidad de dirigir estas medidas solamente contra los cibercafés cuando otras formas de acceso público a Internet (por ejemplo, aeropuertos, bibliotecas y establecimientos públicos con conexiones inalámbricas a Internet) ofrecen a los delincuentes (incluidos los terroristas) las mismas oportunidades de acceso y no están regulados.

445. La cuestión de la medida en que los gobiernos deberían regular los contenidos de Internet relacionados con el terrorismo es problemática, pues exige encontrar el justo equilibrio entre las necesidades de las fuerzas del orden y las consideraciones de derechos humanos, más concretamente, el derecho a la libertad de expresión. Los enfoques de la regulación de los contenidos relacionados con el terrorismo varían, y en tanto que algunos Estados aplican estrictos controles reglamentarios a los proveedores de servicios de Internet y otros proveedores de servicios similares, incluido el uso, en algunos casos, de tecnologías para filtrar o bloquear el acceso a algunos contenidos, otros Estados adoptan un enfoque reglamentario menos estricto, confiando en mayor medida en la autorregulación por parte del sector de la información. La mayoría de los proveedores de servicios de Internet, empresas de hospedaje de sitios web, sitios de intercambio de ficheros y sitios de redes sociales tienen acuerdos de condiciones de servicio que prohíben determinados contenidos; algunos contenidos relacionados con el terrorismo podrían contravenir estas restricciones contractuales.

D. Investigaciones y reunión de datos de inteligencia

446. Las investigaciones eficaces de la actividad en Internet se basan en una combinación de los métodos de investigación tradicionales, el conocimiento de las herramientas disponibles para llevar a cabo actividades ilícitas en Internet y el desarrollo de prácticas dirigidas a descubrir, detener y enjuiciar a los autores de esos actos. Un enfoque proactivo de las estrategias de investigación, complementado con herramientas especializadas que aprovechan los recursos de Internet en evolución, permite determinar de manera eficiente qué datos y servicios son los que tienen más probabilidades de producir el máximo beneficio para la investigación.

447. Hay una amplia gama de aplicaciones y equipos especializados a disposición de los investigadores con la formación técnica adecuada. Siempre que sea posible, habrá que proceder con el debido cuidado, en los casos que exijan obtener pruebas digitales, para emplear procedimientos normalizados de recuperación de datos que promuevan la obtención de la mayor cantidad posible de elementos de prueba y la preservación de la integridad de la fuente de datos y la cadena de custodia para garantizar su admisibilidad en las actuaciones judiciales. Debido a la fragilidad de las pruebas digitales, los más indicados para evaluarlas, obtenerlas y analizarlas son los expertos forenses especialmente capacitados para ello.

E. Cooperación internacional

448. La cooperación internacional eficaz es un factor importante en muchos juicios de actos de terrorismo, incluidos los que entrañan el uso de algún aspecto de Internet por los autores. Los Estados están obligados, en virtud de diversos instrumentos internacionales, regionales, multilaterales y bilaterales relacionados con el terrorismo y la delincuencia organizada transnacional, a establecer políticas y marcos legislativos para facilitar la cooperación internacional eficaz en la investigación y persecución de los actos de terrorismo o los actos graves de delincuencia organizada. En la actualidad, no hay ningún instrumento universal sobre la ciberdelincuencia o el terrorismo que imponga obligaciones específicas a los Estados en relación con la cooperación internacional. Esto es un obstáculo para una cooperación internacional eficaz en algunas investigaciones y juicios relacionados con el terrorismo.

449. Mientras que los canales oficiales de cooperación internacional siguen siendo vitales, en la práctica los canales oficiosos están adquiriendo la misma importancia. Independientemente de la modalidad de cooperación, en muchos casos la confianza entre las respectivas autoridades nacionales es un elemento clave para establecer una cooperación internacional eficaz. Además de la cooperación en virtud de tratados oficiales o instrumentos jurídicos similares, las iniciativas regionales o subregionales, independientes de tratado alguno, encaminadas a fortalecer la cooperación de las fuerzas del orden también son importantes. Los países con intereses comunes de seguridad en determinadas esferas podrían celebrar acuerdos colectivos que previesen el intercambio de información y de inteligencia.

450. La existencia de un marco legislativo nacional que prevea una cooperación internacional efectiva es un elemento fundamental de un marco eficaz para la facilitación de la cooperación internacional en la investigación y el enjuiciamiento de casos de terrorismo. Esta legislación debería incorporar en el derecho interno de un país los principios enunciados en los instrumentos universales contra el terrorismo relacionados con la cooperación y la delincuencia organizada transnacional.

451. Si bien la legislación es un componente fundamental de todo régimen eficaz de cooperación internacional, no es en sí misma la respuesta completa. También es esencial la existencia de una autoridad central, proactiva y dotada de recursos suficientes, capaz de facilitar la asistencia judicial recíproca, utilizando todos los canales disponibles. Es importante también desarrollar y mantener relaciones de confianza con los homólogos extranjeros que colaboran en las investigaciones transfronterizas penales.

452. Además de los canales oficiales de cooperación, las autoridades deben desarrollar y utilizar los canales oficiosos disponibles para la cooperación bilateral. Muchos organismos nacionales encargados de hacer cumplir la ley mantienen una red internacional de puestos de enlace, que prestan valiosa ayuda en la tramitación de las solicitudes de cooperación internacional. En los instrumentos universales contra el terrorismo no hay ninguna referencia expresa a la utilización de equipos conjuntos de investigación; sin embargo, esta estrategia de cooperación está en perfecta consonancia con los principios y el espíritu de los elementos de cooperación internacional en que descansan estos

instrumentos. Algunos países, especialmente en Europa, han adoptado con éxito este enfoque en una serie de investigaciones relacionadas con el terrorismo.

453. A pesar de ciertos progresos, los procedimientos oficiales de asistencia judicial recíproca en materia penal todavía pueden ser trámites largos, con una considerable dosis de burocracia. En los casos de conservación de datos de Internet en poder de proveedores de servicios de Internet situados en otra jurisdicción, las autoridades podrían, en ciertos casos, cooperar directamente con el proveedor de servicios de Internet a título oficioso para preservar dichos datos a los efectos de la investigación o el enjuiciamiento de un delito. En otras situaciones, puede resultar necesario recurrir al ejercicio de un poder coercitivo y una autorización judicial, por ejemplo con respecto a la conservación, el registro y la incautación de datos relacionados con Internet para su presentación y uso como prueba en el proceso penal.

454. Los investigadores y fiscales deben tener plena conciencia de la importancia potencial de estos datos y la necesidad de tomar medidas cuanto antes para mantenerlos en una forma que garantice su admisibilidad como prueba en cualquier procedimiento judicial posterior. En la medida de lo posible, los organismos nacionales encargados de hacer cumplir la ley deberían establecer, ya sea directamente con los proveedores de servicios de Internet o con sus organismos homólogos de otros países, procedimientos claros, con elementos tanto oficiales como oficiosos, destinados a garantizar la retención y obtención expeditiva de los datos necesarios de uso de Internet para las investigaciones penales.

455. Algunos participantes en la reunión del grupo de expertos destacaron el hecho de que la necesidad, por parte de las autoridades nacionales, de proteger datos confidenciales de inteligencia suele representar un obstáculo para el intercambio de información.

456. Cuando se lleva a cabo una investigación en otras jurisdicciones y se desea proceder a la reunión de pruebas digitales, las autoridades deben ser conscientes de las consecuencias que pueden tener sus actos para la soberanía de otros Estados. Siempre que sea posible, las autoridades que consideren medidas de investigación relacionadas con personas u objetos situados en otra jurisdicción deberán notificar y coordinar estas medidas con sus homólogos extranjeros en los países pertinentes.

457. Los datos relacionados con Internet (por ejemplo, el uso por el abonado) constituyen pruebas importantes en muchos casos de terrorismo. En tales casos, las autoridades deben asegurarse de que los datos pertinentes se conserven para su uso posterior como elemento probatorio en las actuaciones. En este sentido, es importante tener en cuenta la distinción entre la “retención” de los datos (datos retenidos por el proveedor de servicios de Internet por obligación reglamentaria) y la “conservación” de los datos (datos que han sido conservados a raíz de una orden o mandato judicial). En muchos países, los proveedores de servicios de Internet están obligados por ley a retener ciertos tipos de datos relacionados con comunicaciones durante un plazo determinado. Sin embargo, a pesar de algunas iniciativas (por ejemplo, a nivel regional en Europa), no existe ningún acuerdo internacional sobre el tipo de datos que deben retener los

proveedores de servicios de Internet ni sobre el plazo de retención. Por consiguiente, a nivel internacional hay una amplia variación en el tipo específico de datos retenidos por los proveedores de servicios de Internet y el plazo durante el que se retienen. Esto puede ser problemático en los casos en que las autoridades necesitan datos de comunicaciones situados en un país, para usar como prueba en un proceso penal que se celebra en otro país.

458. El desarrollo de un marco normativo universalmente aceptado que imponga obligaciones uniformes a todos los proveedores de servicios de Internet en relación con la duración del plazo de retención y el tipo de datos de uso de los abonados que ha de retenerse sería muy beneficioso para los servicios policiales y de inteligencia que investigan casos de terrorismo. A falta de un marco universalmente aceptado para la retención de datos por parte de los proveedores de servicios de Internet, las autoridades deberían determinar, en la etapa más temprana posible, si existen en poder del proveedor de servicios de Internet datos de interés para una investigación y dónde se encuentran, y tomar medidas cuanto antes a fin de preservarlos para su posible uso como prueba.

459. En la medida de lo posible, las autoridades deberían establecer relaciones o acuerdos officiosos con los proveedores de servicios de Internet (tanto nacionales como extranjeros) que puedan tener en su poder datos de interés para las fuerzas del orden acerca de los procedimientos para la obtención de esos datos en las investigaciones policiales. En ausencia de tales procedimientos officiosos, durante las investigaciones las autoridades deberían establecer enlace cuanto antes con sus homólogos extranjeros, de ser necesario por los canales oficiales, y obtener las autorizaciones judiciales necesarias para la conservación de los datos.

460. Desde el punto de vista probatorio, los casos de terrorismo que requieren investigaciones transfronterizas añaden una dificultad más a lo que ya puede ser una tarea compleja para investigadores y fiscales, lo que exige que se aseguren de que los métodos seguidos para reunir las pruebas (posiblemente en uno o más países) y presentarlas como tales en un juicio llevado a cabo en otra jurisdicción, estén en plena conformidad con las leyes y los principios aplicables de todas las jurisdicciones pertinentes.

461. El requisito de la doble incriminación (que los hechos que motivan las solicitudes de extradición y asistencia judicial recíproca constituyan delitos en los dos Estados), que figura comúnmente en muchos instrumentos multilaterales y bilaterales relacionados con el terrorismo y la delincuencia organizada transnacional, puede presentar dificultades en las causas penales, incluidas las relacionadas con el terrorismo, que requieren cierta cooperación internacional.

462. Los casos de terrorismo en que ciertos elementos del delito se perpetran por Internet pueden presentar complejas cuestiones de competencia, especialmente en los casos en que el presunto delincuente se encuentra en un país y utiliza los sitios de Internet o los servicios de proveedores de servicios de Internet situados en otro país para llevar a cabo actos que son elementos de un delito. Ha habido varios casos de personas que residen en un país y crean y administran sitios web en otro país para promover la yihad y otros actos violentos relacionados con el terrorismo.

463. No hay normas vinculantes conforme al derecho internacional que traten de la cuestión de cómo han de proceder los Estados en los casos en que haya más de un Estado con competencia para perseguir un delito que implique al mismo sospechoso. Por lo general, las autoridades nacionales sopesan los factores pertinentes, incluido el grado de conectividad entre las distintas jurisdicciones y el presunto delito, para determinar si se debe hacer valer y ejercer la competencia en un caso particular. En los casos de conflictos de competencia, la comunicación y colaboración desde un primer momento entre las autoridades centrales (muchas veces, las fiscalías nacionales) es importante para la resolución de estas cuestiones.

464. La legislación nacional de protección de datos o sobre privacidad restringe con frecuencia la capacidad de los servicios de policía y de inteligencia para compartir información con los homólogos tanto nacionales como extranjeros. El logro de un equilibrio razonable entre el derecho humano a la privacidad y el interés legítimo del Estado de investigar y perseguir los delitos es un problema permanente para los gobiernos y, en algunos casos, en particular los que entrañan respuestas al terrorismo, este conflicto de intereses ha sido motivo de preocupación.

F. El proceso penal

465. Parte integrante del marco jurídico universal contra el terrorismo, la Estrategia global de las Naciones Unidas contra el terrorismo, es la obligación impuesta a los Estados de negar refugio seguro y someter a juicio a los autores de actos de terrorismo, dondequiera que los cometan. Además de la existencia del necesario marco legislativo, la capacidad institucional de los organismos judiciales nacionales de respetar el estado de derecho en los juicios de casos relacionados con el terrorismo, de conformidad con los derechos humanos de los sospechosos y acusados en virtud de las normas internacionales de derechos humanos, es parte integrante de una respuesta eficaz de la justicia penal al terrorismo.

466. Frecuentemente, los fiscales no se limitan a participar en la fase de enjuiciamiento de los casos de terrorismo sino que también desempeñan un papel directo en la fase de la investigación, prestando asesoramiento jurídico y estratégico sobre cuestiones que influirán en el resultado de cualquier acción judicial ulterior. Es probable que desempeñen su función como parte de un equipo multidisciplinario y multijurisdiccional. El alto nivel de confianza, coordinación y comunicación, vital para la cooperación eficaz a nivel internacional, también tiene que existir entre los organismos nacionales de mantenimiento del orden, de inteligencia y de enjuiciamiento.

467. Mientras que las nuevas técnicas de investigación ofrecen mayores oportunidades a las autoridades de combatir las actividades terroristas en Internet, también conllevan riesgos jurídicos que los fiscales deben tener muy presentes. Las diferencias entre las legislaciones nacionales relativas a la obtención y admisibilidad de las pruebas significan que estos riesgos son mayores cuando los procedimientos que permitieron obtener las pruebas tuvieron lugar en una jurisdicción diferente de aquella en la que se desarrolla el proceso.

468. En la mayoría de los países, los fiscales ejercen amplia discreción en cuanto a si ha de iniciarse la acción penal y los cargos que han de imputarse. Estas decisiones suelen adoptarse de acuerdo con directrices o códigos que han sido concebidos para garantizar el ejercicio imparcial, transparente y consecuente de esa facultad tan importante, y suelen establecer umbrales basados en la suficiencia probatoria y el interés público.

469. El objetivo principal de las investigaciones relacionadas con el terrorismo es la seguridad pública. En algunos casos, las autoridades deben intervenir para impedir la comisión de actos terroristas antes de que haya datos suficientes para iniciar un proceso judicial por los actos terroristas que las autoridades sospechan que se están planeando.

470. En estas situaciones, las autoridades pueden verse obligadas a invocar otros delitos como base jurídica de sus actos, como los delitos, entre otros, de instigación, con-fabulación, asociación ilícita, o prestación de apoyo material a terroristas, y no los delitos en sí relacionados con los actos terroristas que están planeando. Pueden invocarse también otras disposiciones penales generales relacionadas con el fraude o la posesión o el uso de artículos ilegales (por ejemplo, documentos de identidad o de viaje falsos, armas) para desbaratar o socavar las actividades de grupos terroristas antes de que lleguen a ejecutar los actos o atentados planeados.

471. En muchos casos de terrorismo, las pruebas presentadas por la fiscalía se basan en la inteligencia reunida. La integración de las actividades de inteligencia en los sistemas de justicia penal sigue siendo un problema fundamental para las autoridades que combaten el terrorismo, o, dicho de otro modo, ¿cómo pueden las autoridades proteger la confidencialidad de la inteligencia en que se basan las pruebas al tiempo que cumplen sus obligaciones de garantizar un juicio imparcial y una defensa eficaz de los acusados, incluida la obligación de revelar todos los elementos importantes de la acusación a la defensa?

472. En los casos de terrorismo en que se usan computadoras o Internet, las pruebas digitales son parte importante de la acusación. El uso de tales pruebas invariablemente da lugar a cuestiones relacionadas con la admisibilidad. Es de suma importancia proceder con extremo cuidado durante toda la investigación y el enjuiciamiento del caso para asegurarse de que los métodos de obtención, conservación, análisis y presentación de las pruebas digitales estén en plena conformidad con las normas pertinentes respecto de las pruebas o los procedimientos y sigan las buenas prácticas establecidas.

473. El ministerio público tendrá que convencer al tribunal de la confiabilidad de las pruebas digitales, incluidos los métodos de reunión, análisis y producción. Los procedimientos seguidos para preservar la integridad de las pruebas se conocen por el nombre de “cadena de custodia” o “cadena de pruebas”. Cuando esas pruebas se recogen en una jurisdicción para ser usadas en juicio en otra jurisdicción, la situación es mucho más complicada y requiere una atención extrema por parte de investigadores y fiscales. En caso de que las autoridades descubran la existencia o la ubicación, o ambas cosas, de pruebas digitales de interés, deberán explorar los medios (oficiales y extraoficiales)

de obtenerlas y preservarlas con fines probatorios. El método elegido deberá garantizar la admisibilidad de las pruebas en el país donde se lleve a cabo el juicio.

474. Los principios jurídicos y los procedimientos relacionados con la obtención y admisibilidad de las pruebas en los procesos penales suelen variar de una jurisdicción a otra. Parte importante de la labor de las autoridades en las investigaciones transfronterizas implica la “mediación” de diferentes aspectos de las pruebas. Este proceso puede ser complejo y largo, pero es un factor crítico en el éxito de los juicios. Cualquier deficiencia legal de los métodos por los cuales se recogieron, preservaron, transmitieron o produjeron las pruebas utilizadas en el juicio será impugnada en última instancia, casi con certeza, por la defensa.

475. En los casos de terrorismo, los fiscales se suelen ver obligados a presentar pruebas periciales para demostrar algún aspecto especializado de la causa. Las esferas en que suele necesitarse el testimonio pericial incluyen las de la tecnología y las comunicaciones, y las de las ideologías, actividades y estructura orgánica de los grupos terroristas. Es muy posible que los fiscales necesiten el testimonio de varios peritos. Por lo general, los casos que requieren testimonio pericial se desarrollan en tres etapas o fases: *a)* clara determinación de cuáles son los problemas (y su alcance) que requieren dictamen pericial; *b)* selección de un perito cualificado; y *c)* necesidad de asegurarse de que el perito cualificado emplee medios admisibles.

476. Los fiscales deben tratar de determinar lo antes posible cuáles son las cuestiones que probablemente requieran el testimonio de peritos y contratarlos para que lleven a cabo los análisis necesarios, en su caso, proporcionándoles una orientación clara sobre las normas procesales o probatorias fundamentales. Al seleccionar a los peritos, los fiscales deben considerar si han de usar peritos gubernamentales o no gubernamentales. Si bien el uso de testigos gubernamentales puede ofrecer ventajas, a veces resulta preferible contratar a peritos no gubernamentales, especialmente en los casos en que las pruebas se basan en fuentes o métodos de inteligencia confidenciales. La búsqueda de un perito idóneo, sobre todo en campos altamente especializados, puede suponer una seria dificultad para los países menos desarrollados. Cuando proceda, los peritos deberán seguir y aplicar las buenas prácticas reconocidas en el campo particular en que se los ha llamado a declarar. Debido a la complejidad de algunos testimonios periciales, se deben considerar formas innovadoras de presentar en juicio pruebas complejas, de manera que sea fácil de entender para jueces, jurados o jueces de hecho. Es importante que el fiscal tenga un buen conocimiento práctico de la materia.

477. La complejidad de muchos procesos relacionados con el terrorismo, en particular los que requieren cooperación internacional o contienen elementos muy técnicos, hace que sea muy aconsejable poner esas causas en manos de un equipo de fiscales. A fin de velar por la adopción de un enfoque integrado de respeto del estado de derecho y de preservación de la integridad de las respuestas de la justicia penal al terrorismo, los países deben contar con mecanismos sólidos y permanentes para fortalecer la capacidad de los fiscales de aplicar la legislación nacional contra el terrorismo y cumplir con las obligaciones internacionales de cooperación conexas. En los países donde el riesgo de actividad terrorista es alto y la capacidad institucional del ministerio público y otros

servicios de la justicia penal es baja, debe atribuirse una alta prioridad a la formación de especialistas dentro de estos organismos, no solo en cuanto al enjuiciamiento, sino también con respecto a los procedimientos de cooperación internacional.

G. Cooperación del sector privado

478. Si bien la responsabilidad de contrarrestar el uso de Internet con fines terroristas incumbe, en última instancia, a los Estados Miembros, la cooperación de las principales entidades interesadas del sector privado es de importancia decisiva para la ejecución eficaz. La colaboración proactiva con las partes interesadas del sector privado tales como los proveedores de servicios, los sitios web que hospedan contenido generado por los usuarios y los buscadores de Internet, seguirá desempeñando un papel importante en el control de la disponibilidad de contenidos relacionados con el terrorismo difundidos por Internet.

479. Sería beneficioso el establecimiento de asociaciones entre el sector público y el privado en relación con la regulación de Internet para frustrar su uso con fines terroristas. Se han emprendido con éxito iniciativas similares con respecto a otras esferas de la lucha contra el terrorismo y contra la ciberdelincuencia en general. Estas iniciativas ofrecen un foro para el diálogo oficial y oficioso entre los homólogos de los sectores público y privado, además de apoyar actividades tales como la ejecución de programas de capacitación conjuntos, que pueden ayudar a superar las barreras a la comunicación, fomentar la confianza y la comprensión, y desarrollar prácticas armonizadas entre los miembros activos de la asociación.



UNODC

Oficina de las Naciones Unidas
contra la Droga y el Delito

Centro Internacional de Viena, Apartado postal 500, 1400 Viena, Austria
Tel.: (+43-1) 26060-0, Fax: (+43-1) 26060-5866, www.unodc.org

Publicación de las Naciones Unidas
Impreso en Austria



V.12-57355—Julio de 2013