LUCHA ANTITERRORISTA EN EL CIBERESPACIO

Los terroristas y grupos terroristas no solo explotan Internet y los medios sociales para cometer actos terroristas, sino también para facilitar una amplia gama de actividades con fines terroristas, como la incitación, la radicalización, la captación, el adiestramiento, la planificación, la recopilación de información, las comunicaciones, la preparación y la financiación. La pandemia de COVID-19, durante la cual se produjeron confinamientos e imposiciones de distanciamiento físico en muchos Estados Miembros, también dio lugar a un aumento espectacular del uso de Internet, lo que suscitó una gran preocupación por el uso indebido de las tecnologías de la información y las comunicaciones (TIC) por parte de terroristas y grupos terroristas, así como de personas y grupos que propugnaban ideologías de extrema derecha (o de motivación racial o étnica). En su labor para abordar estas cuestiones subyacentes, el Comité contra el Terrorismo se guía por varias resoluciones del Consejo de Seguridad, entre ellas:

- La **resolución 1373 (2001) del Consejo de Seguridad**, aprobada poco después de los atentados del 11 de septiembre de 2001 contra los Estados Unidos y en la que se exhorta a todos los Estados Miembros a encontrar medios para intensificar y agilizar el intercambio de información operacional sobre la utilización de las TIC por grupos terroristas y reprimir el reclutamiento de terroristas.
- La **resolución 1624 (2005) del Consejo de Seguridad**, en la que se insta a adoptar las medidas necesarias y adecuadas, en cumplimiento de las obligaciones de derecho internacional de los Estados Miembros, para prohibir por ley la incitación a cometer actos terroristas e impedir dichas conductas.
- La **resolución 2129 (2013) del Consejo de Seguridad**, en la que se encarga a la DECT que siga ocupándose de la utilización de las TIC en las actividades relacionadas con el terrorismo, en consulta con los Estados Miembros, las organizaciones internacionales, regionales y subregionales, el sector privado y la sociedad civil, y que asesore al Comité contra el Terrorismo sobre otros enfoques.
- La **resolución 2178 (2014) del Consejo de Seguridad**, relativa a la reducción de la afluencia de combatientes terroristas extranjeros, en la que se exhorta a que los Estados Miembros cooperen entre sí al adoptar medidas nacionales para impedir que los terroristas se aprovechen de tecnologías, comunicaciones y recursos para incitar al apoyo de actos terroristas, respetando al mismo tiempo los derechos humanos y las libertades fundamentales y cumpliendo otras obligaciones dimanantes del derecho internacional.
- **En sus resoluciones 2322 (2016), 2331 (2016), 2341 (2017) y 2396 (2017)**, el Consejo de Seguridad pide a los Estados que reúnan y conserven pruebas digitales de manera que se puedan realizar investigaciones y enjuiciamientos para que los responsables de atentados terroristas rindan cuentas de ellos.
- **En las resoluciones del Consejo de Seguridad 2341 (2017), 2354 (2017), 2395 (2017) y 2396 (2017)** se reconoce la necesidad de desarrollar alianzas público-privadas mediante una cooperación voluntaria para hacer frente a la explotación de las TIC con fines terroristas, incluso en el desarrollo de contraargumentos y soluciones tecnológicas, respetando al mismo tiempo los derechos humanos y las libertades fundamentales, y cumpliendo el derecho nacional e internacional. En la resolución 2395 (2017) del Consejo de Seguridad se reconoce la labor de la DECT en este sentido.
- **En la resolución 2354 (2017) del Consejo de Seguridad** se establecen directrices para aplicar un marco internacional amplio en materia de contraargumentos y difundir ampliamente alternativas positivas y creíbles para los grupos vulnerables a los mensajes extremistas.
- **En la resolución 2462 (2019) del Consejo de Seguridad** se observa el uso de plataformas de financiación colectiva para recaudar fondos con fines terroristas, así como la utilización de métodos de pago emergentes como las tarjetas de prepago, los sistemas de pago por telefonía móvil o los activos virtuales para trasladar y transferir dichos fondos. También se exhorta a que se evalúen y afronten los posibles riesgos asociados con los activos virtuales y los nuevos instrumentos financieros.

Además, el Comité contra el Terrorismo ha elaborado orientaciones en este ámbito para los Estados Miembros a través de los **Principios Rectores de Madrid de 2015 (S/2015/939) y la adición de 2018 (S/2018/1177)** sobre los combatientes terroristas extranjeros. Los principios rectores 13, 14, 33, 43 y 44 se centran en los métodos para vigilar y estudiar los contenidos relativos al terrorismo transmitidos a través de Internet y otras tecnologías de la comunicación; revisar las leyes y mecanismos nacionales de asistencia judicial recíproca ante el aumento de las solicitudes de datos digitales; y reunir datos y pruebas digitales en casos relacionados con los combatientes terroristas extranjeros. Siguiendo la orientación sobre políticas del Comité, el trabajo de la DECT sobre las TIC se centra en cuatro pilares: i) integración de las TIC en las visitas de evaluación realizadas en nombre del Comité para

evaluar la aplicación por los Estados Miembros de las resoluciones pertinentes del Consejo de Seguridad; ii) el fomento de la autorregulación del sector y las alianzas público-privadas; iii) el refuerzo de la cooperación internacional para el acceso legal a los contenidos digitales; y iv) la promoción de técnicas de contrapropaganda, incluso en línea.

VISITAS DE EVALUACIÓN DEL COMITÉ CONTRA EL TERRORISMO A LOS ESTADOS MIEMBROS

El uso de las TIC con fines terroristas es una de las áreas temáticas clave de las visitas de evaluación a los Estados Miembros realizadas en nombre del Comité contra el Terrorismo por su Dirección Ejecutiva (DECT), y durante la pandemia de COVID-19 también se integró esta área temática en las visitas híbridas realizadas en ese contexto. Las cuestiones relacionadas con las TIC se exponen en la guía técnica para la aplicación de la resolución 1373 (2001) del Consejo de Seguridad y otras resoluciones pertinentes (S/2017/716) y en el documento marco actualizado para las visitas del Comité a los Estados Miembros con el fin de supervisar, promover y facilitar la aplicación de las resoluciones del Consejo de Seguridad 1373 (2001), 1624 (2005), 2178 (2014), 2396 (2017), 2462 (2019) y 2482 (2019) y otras resoluciones pertinentes del Consejo (S/2020/731). Las cuestiones específicas relacionadas con el uso indebido de las TIC con fines terroristas que se debaten con los Estados Miembros durante las visitas de evaluación incluyen:

- Marcos normativos y de políticas relativos a las TIC
- Legislación contra el uso indebido de las TIC con fines terroristas
- Capacidad de utilizar técnicas especiales de investigación para vigilar la utilización de las TIC con fines terroristas
- Métodos de identificación de contenidos y actividades terroristas prácticas operacionales para bloquear, filtrar y eliminar contenidos en línea relacionados con el terrorismo
- Cooperación con el sector privado y la sociedad civil (alianzas público-privadas) para contrarrestar el uso de las TIC con fines terroristas, incluso mediante soluciones tecnológicas
- Utilización de pruebas digitales para llevar a los terroristas ante la justicia, incluido el acceso a pruebas digitales almacenadas en otra jurisdicción (legislación, estructura nacional, nivel de aplicación de la ley y asistencia recíproca en asuntos penales)
- Políticas para la seguridad de las infraestructuras críticas y la resiliencia frente a las actividades maliciosas de los terroristas, incluso mediante el uso de las TIC
- Aspectos relacionados con los derechos humanos de las medidas de lucha contra el terrorismo adoptadas por los Estados Miembros, incluidas las salvaguardias adecuadas para la libertad de expresión en relación con las TIC.

Las cuestiones relacionadas con las TIC (pruebas digitales, protección de infraestructuras críticas, incitación en línea y moderación en línea, entre otras) también se han incluido en la sinopsis de la evaluación de la aplicación y el estudio detallado de la aplicación en formato electrónico (e-DIS), los instrumentos de estudio recientemente actualizados del Comité y su Dirección Ejecutiva, que están alojados en un nuevo portal de evaluación y análisis basado en la nube.

COLABORACIÓN CON EL SECTOR PRIVADO

Desde 2014, la DECT, siguiendo la orientación sobre políticas del Comité, ha colaborado activamente con el sector privado en el ámbito de las TIC. En 2017, esta colaboración se formalizó en una alianza público-privada denominada ***Tech Against Terrorism***. Esta iniciativa, en la que participan numerosos asociados de los Gobiernos, el sector privado, asociaciones comerciales, la sociedad civil, el mundo académico y foros de múltiples partes interesadas, tiene por objeto ayudar al sector tecnológico mundial a hacer frente a la explotación terrorista de las tecnologías, respetando al mismo tiempo los derechos humanos. Sobre la base de consultas a escala mundial con

partes interesadas clave, Tech Against Terrorism trabaja con el sector tecnológico mundial para compartir buenas prácticas, incluidas políticas, directrices, material didáctico, talleres prácticos y otras herramientas. Otra característica fundamental es el apoyo y el saber hacer brindado por las grandes plataformas a plataformas más pequeñas y empresas emergentes para evitar que se vean explotadas por terroristas.

Además, la DECT ha sido un asociado importante del ***Foro Mundial de Internet para Contrarrestar el Terrorismo***, fundado por Facebook, Google, Microsoft y Twitter en 2017, que es ahora una ONG independiente. La DECT es observadora permanente del comité consultivo independiente del Foro. Tech Against Terrorism trabaja en estrecha colaboración con el Foro Mundial de Internet para Contrarrestar el Terrorismo en el apoyo de las pequeñas plataformas y el desarrollo de soluciones tecnológicas. Desde 2016, los miembros del Foro han modificado sus términos de uso para prohibir la publicación de contenido terrorista o en apoyo de organizaciones incluidas en la Lista Consolidada de Sanciones del Consejo de Seguridad de las Naciones Unidas. En sus resoluciones 2617 (2021), 2395 (2017) y 2396 (2017), el Consejo tomó nota del Foro Mundial de Internet para Contrarrestar el Terrorismo y de la iniciativa Tech Against Terrorism y pidió que continuaran sus esfuerzos encaminados a fomentar la colaboración público-privada para desbaratar la capacidad de los terroristas de utilizar Internet con fines terroristas.

LUCHA CONTRA EL EXTREMISMO VIOLENTO Y LOS ARGUMENTOS TERRORISTAS

Los grupos terroristas han logrado hacer un uso exitoso de la propaganda con múltiples fines, entre ellos el reclutamiento y la radicalización violenta. La resolución 2354 (2017) del Consejo de Seguridad se basa en la declaración de la Presidencia del Consejo de 11 de mayo de 2016 (S/PRST/2016/6) y en el Marco Internacional Amplio para Refutar los Argumentos Terroristas (S/2017/375), que aborda las medidas jurídicas y de aplicación de la ley, las alianzas público-privadas y la formulación de contraargumentos. La resolución establece una serie de directrices que destacan, entre otros factores, que las actividades de las Naciones Unidas para refutar los argumentos terroristas deben basarse en la Carta de las Naciones Unidas; que los Estados Miembros tienen la responsabilidad primordial de contrarrestar los actos de terrorismo y el extremismo violento que conduce al terrorismo; que las entidades pertinentes de las Naciones Unidas deben aumentar la coordinación con los donantes y los receptores de capacitación contra el terrorismo, así como la coherencia de esas actividades; que las medidas y los programas para refutar los argumentos terroristas deben adaptarse a los distintos contextos; que todas las medidas deben ajustarse a las obligaciones que les incumben a los Estados Miembros en virtud del derecho internacional, en particular el derecho internacional de los derechos humanos, el derecho internacional de los refugiados y el derecho internacional humanitario; y que es necesario seguir investigando los factores que promueven el terrorismo y el extremismo violento a fin de elaborar programas más centrados para refutar los argumentos terroristas.

En su resolución 2354 (2017), el Consejo solicita al Comité contra el Terrorismo que siga identificando y compilando las buenas prácticas existentes para refutar los argumentos terroristas, en coordinación con la Oficina del Equipo Especial (el Equipo Especial de las Naciones Unidas sobre la Ejecución de la Lucha contra el Terrorismo), ahora la Oficina de Lucha contra el Terrorismo (OLCT) y, cuando proceda, en consulta con otras entidades pertinentes no pertenecientes a las Naciones Unidas. El Comité contra el Terrorismo también seguirá examinando las medidas jurídicas adoptadas por los Estados para mejorar la aplicación, desarrollar nuevas alianzas público-privadas, llevar a cabo actividades de divulgación dirigidas a las organizaciones de la sociedad civil y los agentes religiosos, y colaborar con los miembros de la Red Mundial de Investigación sobre la Lucha Antiterrorista de la DECT y otras entidades para medir el impacto y la eficacia de los contraargumentos.

Por consiguiente, en sus evaluaciones de la aplicación por los Estados Miembros de las resoluciones pertinentes del Consejo de Seguridad, el Comité y la DECT dedican especial atención a las medidas adoptadas por los Estados para instituir programas y estrategias de lucha contra la incitación, de conformidad con la resolución 1624 (2005); para tipificar como delito la incitación y luchar contra los argumentos terroristas, de conformidad con la resolución 2354 (2017); y para combatir el extremismo violento, de conformidad con la resolución 2178 (2014) y otras. Cuando existen deficiencias, el Comité y la DECT intentan conectar a los Estados con proveedores de asistencia técnica para desarrollar nuevas iniciativas en los ámbitos correspondientes.

El Comité y la DECT se han comprometido a coordinar sus esfuerzos con los realizados en apoyo de la Estrategia Global de las Naciones Unidas contra el Terrorismo, en particular mediante la participación de la DECT en el Pacto Mundial de Coordinación de la Lucha Antiterrorista de las Naciones Unidas.

PRUEBAS DIGITALES

Una parte vital de los esfuerzos antiterroristas es la promoción de respuestas eficaces de la justicia penal basadas en el estado de derecho. En la práctica, los Estados Miembros se enfrentan a grandes dificultades para la obtención de pruebas admisibles que puedan utilizarse para enjuiciar a los sospechosos de terrorismo y lograr que sean condenados en procedimientos judiciales. La situación de los combatientes terroristas extranjeros, y en particular la de los que regresan y se reasientan, representa un reto especialmente grave. Dado que la información relacionada con las actividades de los combatientes terroristas extranjeros suele encontrarse en el campo de batalla, puede resultar inaccesible para los fiscales e investigadores civiles. Por lo tanto, el enjuiciamiento de los combatientes terroristas extranjeros puede depender del uso de pruebas digitales o procedentes de Internet y requerir formas de cooperación judicial que no están previstas en los marcos jurídicos establecidos. A la vista de los retos, y en virtud de las resoluciones 2322 (2016), 2331 (2016), 2341 (2017) y 2396 (2017) y de los mencionados principios rectores sobre los combatientes terroristas extranjeros (Principios Rectores de Madrid) y la adición de 2018, la DECT, junto con la Asociación Internacional de Fiscales (IAP) y la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), puso en marcha una iniciativa mundial para, entre otras cosas, reforzar la capacidad de las autoridades centrales, los fiscales y los investigadores para preservar y obtener pruebas electrónicas en el marco de las investigaciones transfronterizas de lucha contra el terrorismo.

PRIVACIDAD Y PROTECCIÓN DE LOS DATOS

A medida que la lucha contra el terrorismo plantea cada vez más retos relacionados con la privacidad y la protección de los datos, los expertos perciben una falta de marcos jurídicos y orientaciones sobre protección de datos para las empresas privadas y los gobiernos en los que se aborden cuestiones técnicas como los criterios legales de inclusión, las políticas de conservación o eliminación de datos, el procesamiento, el intercambio, la prevención del uso indebido y la seguridad de los datos, la validación y la supervisión. Esto crea un gran obstáculo para la cooperación internacional y el intercambio internacional de datos, ya que muchos Estados tienen prohibido, de conformidad con su derecho interno respectivo, divulgar datos protegidos y personales a Estados que tienen regímenes de protección de datos más débiles. Además, los nuevos avances, como los progresos en el campo de la inteligencia artificial (por ejemplo, el aprendizaje automático) y la mayor dependencia de herramientas impulsadas por esta tecnología hacen necesario el desarrollo de orientaciones. La DECT está codirigiendo, junto con la UNODC y la OLCT y en el marco del Grupo de Trabajo sobre Justicia Penal, Respuestas Jurídicas y Lucha contra la Financiación del Terrorismo del Pacto Mundial de Coordinación de la Lucha Antiterrorista, un proyecto sobre la elaboración de disposiciones legislativas recomendadas y un compendio de buenas prácticas vigentes sobre normas de protección de datos para facilitar la cooperación internacional en la lucha contra el terrorismo.

INTELIGENCIA ARTIFICIAL

En la lucha antiterrorista está muy extendido el uso de la inteligencia artificial (IA), desde la moderación automática de contenidos por los proveedores de servicios de comunicaciones hasta el uso de datos biométricos. El aprendizaje automático y la adopción automatizada de decisiones se consideran herramientas de vigilancia e investigación sumamente útiles, pero también graves amenazas para el disfrute de los derechos civiles y políticos (entre otros, con respecto a la privacidad y la libertad de expresión y en relación con la discriminación racial y de género). La DECT ha colaborado con varios asociados que trabajan en este ámbito, en particular el Instituto Interregional de las Naciones Unidas para Investigaciones sobre la Delincuencia y la Justicia (UNICRI) y el Foro Económico Mundial. Además, la DECT ha seguido la evolución del uso de algoritmos basados en IA por parte de las plataformas tecnológicas (incluidas las empresas que forman parte del Foro Mundial de Internet para Contrarrestar el Terrorismo) a fin de apoyar sus iniciativas de moderación de contenidos. La Hoja de Ruta del Secretario General para la Cooperación Digital señala la importancia de la IA para la promoción de la paz y destaca la labor de la DECT en varios asuntos relacionados con la IA. La DECT asesora a la Oficina Ejecutiva del Secretario General sobre la aplicación de dicha Hoja de Ruta.

NUEVOS INSTRUMENTOS FINANCIEROS

Las nuevas tecnologías dotadas de estructuras descentralizadas y distribuidas, como la tecnología de cadenas de bloques, pueden ser utilizadas y explotadas por diferentes partes interesadas para intercambiar, transferir, retirar o contabilizar diversas clases de activos fuera de las redes financieras tradicionales. Los activos virtuales como Bitcoin permiten realizar transferencias internacionales de fondos de forma anónima, y hay constancia de que esto se viene utilizando cada vez más para financiar el terrorismo. El uso de métodos de financiación colectiva también representa un riesgo conocido de financiación del terrorismo a nivel mundial. La financiación colectiva es la manera en que empresas, organizaciones y personas recaudan fondos por Internet, por medio de donaciones o inversiones realizadas por múltiples personas. En su labor de lucha contra la financiación del terrorismo, la DECT ha prestado cada vez más atención a los riesgos de financiación del terrorismo asociados a las nuevas tecnologías, como los activos virtuales y las plataformas de financiación colectiva, así como a la necesidad de establecer alianzas eficaces con el sector privado. La DECT vigila y analiza las últimas tendencias en este ámbito a través de su diálogo con los Estados Miembros (también en el marco de sus evaluaciones de la lucha contra la financiación del terrorismo); su participación en los foros de expertos pertinentes (incluidos los proyectos especializados del Grupo de Acción Financiera (GAFI)); intercambios con el Equipo de Apoyo Analítico y Vigilancia de las Sanciones dimanante de las resoluciones 1526 (2004) y 2253 (2015) relativas al EIIL (Dáesh), Al-Qaida y los talibanes y personas y entidades asociadas, así como con otros asociados pertinentes; consultas con el sector privado y organizaciones de la sociedad civil; y sus investigaciones en curso (en particular a través de su Red Mundial de Investigación). De conformidad con la resolución 2462 (2019), la DECT también trabaja con los Estados para que apliquen a los proveedores de servicios de activos virtuales reglamentos y medidas de vigilancia y supervisión contra la financiación del terrorismo basados en la evaluación de los riesgos.