UNITED NATIONS
OFFICE OF COUNTER-TERRORISM
Programme Office in Doha

Parliamentary Engagement
in Preventing and Countering Terrorism

OSCE PA
Organization for Security and Co-operation in Europe
PARLIAMENTARY ASSEMBLY

مجلس الشورى
The Shura Council
State of Qatar • دولة قطر

DOCUMENTO DE RESULTADOS

CUARTO DIÁLOGO PARLAMENTARIO SOBRE POLÍTICAS DE LUCHA CONTRA EL USO DE LA INTELIGENCIA ARTIFICIAL Y LAS NUEVAS TECNOLOGÍAS CON FINES TERRORISTAS

Roma, Italia
5 de diciembre de 2024

Este documento no constituye el acta de las conclusiones oficiales ni es un registro exhaustivo de todos los asuntos abordados durante el Diálogo Parlamentario sobre Políticas. Su finalidad es aportar una recopilación de cuestiones importantes, lecciones clave y recomendaciones a modo de referencia para el futuro. Aunque la Oficina de Lucha contra el Terrorismo (OLCT) de las Naciones Unidas hace todos los esfuerzos necesarios por asegurar la precisión y la pertinencia de la información presentada, no asume ninguna responsabilidad ni ofrece ninguna garantía, explícita ni implícita, sobre la exhaustividad, exactitud o fiabilidad del contenido. Las opiniones y recomendaciones aquí recogidas se presentan únicamente como referencia y no deben interpretarse como definitivas ni completas.

Este documento es una traducción no oficial proporcionada únicamente con fines informativos. En caso de discrepancias o ambigüedades, prevalecerá la versión original en inglés.

RESUMEN

La Oficina del Programa sobre la Colaboración Parlamentaria en la prevención y la lucha contra el terrorismo de la Oficina de Lucha contra el Terrorismo de las Naciones Unidas (OLCT) y la Dependencia de Ciberseguridad y Nuevas Tecnologías de la OLCT, con el apoyo del Consejo de la Shura del Estado de Qatar y en colaboración con la Asamblea Parlamentaria de la Organización para la Seguridad y la Cooperación en Europa (AP OSCE), organizaron el Cuarto Diálogo Parlamentario sobre Políticas, dedicado al tema "La lucha contra el uso de la IA y las nuevas tecnologías con fines terroristas". El encuentro, celebrado en el Parlamento italiano en Roma el 5 de diciembre de 2024, reunió a más de 70 participantes presencialmente y una decena en línea, incluidos representantes de asambleas parlamentarias y de parlamentos nacionales de África, Asia y Europa, además de destacados expertos en la materia de agencias de las Naciones Unidas, organizaciones internacionales de investigación y centros académicos.

Participaron representantes de catorce asambleas parlamentarias, entre ellas, la Unión Parlamentaria Africana (UPA), la Unión Interparlamentaria Árabe (UIP Árabe), el Parlamento Árabe, la Asamblea Interparlamentaria de la ASEAN (AIPA), la Asamblea Parlamentaria de la Francofonía (APF); el Parlamento Europeo (PE); la Asamblea Interparlamentaria de Naciones Miembros de la Comunidad de Estados Independientes (AIP CEI), la Asamblea Parlamentaria de la Cooperación Económica del Mar Negro (PABSEC), la Asamblea Parlamentaria del Consejo de Europa (APCE), la Asamblea Parlamentaria del Mediterráneo (APM), la Asamblea Parlamentaria de la Organización para la Seguridad y la Cooperación en Europa (AP OSCE), la Unión Parlamentaria de los Estados Miembros de la Organización de Cooperación Islámica (UPCI), la Asamblea Parlamentaria de la Organización de los Estados Túrquicos (TURKPA) y el Foro Parlamentario de la Comunidad de África Meridional para el Desarrollo (FP SADC). También hubo representantes del Consejo de la Shura del Estado de Qatar.

El panel de expertos contó con la presencia de representantes de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), la Dirección Ejecutiva del Comité contra el Terrorismo (DECT) del Conejo de Seguridad de las Naciones Unidas, la Cámara de los Diputados del Parlamento de Italia, la Agencia Nacional de Ciberseguridad italiana y otras organizaciones internacionales y laboratorios de ideas, como la fundación Geneva Centre for Security Policy, Mythos Labs, el instituto Centre for Global Studies, la Asamblea Parlamentaria del Mediterráneo (APM) y el Comité Especial para la Lucha contra el Terrorismo de la Asamblea Parlamentaria de la OSCE.

El diálogo político incluyó tres sesiones principales:

1. Las amenazas y los retos mundiales y regionales relacionados con el uso de la inteligencia artificial (IA) y otras nuevas tecnologías con fines terroristas;
2. Buenas prácticas parlamentarias regionales e internacionales para la prevención y la lucha contra el uso de la IA y otras nuevas tecnologías con fines terroristas;
3. El marco jurídico internacional para la prevención y la lucha contra el uso de la IA y otras nuevas tecnologías con fines terroristas.

El diálogo finalizó con varias recomendaciones clave relativas a la prevención y la lucha contra el uso de la IA y otras tecnologías emergentes por parte de organizaciones terroristas y extremistas, enfatizando la función primordial de los parlamentos nacionales y las asambleas parlamentarias multilaterales en este empeño.

INFORMES DE SESIÓN

SESIÓN I. Las amenazas y los retos mundiales y regionales relacionados con el uso de la inteligencia artificial y otras nuevas tecnologías con fines terroristas

La sesión presentó una completa perspectiva de los desafíos actuales y emergentes para la seguridad mundial y regional derivados del uso indebido de la IA y otras nuevas tecnologías para fines terroristas. Los participantes pusieron de relieve el efecto transformador de estas tecnologías en la naturaleza cambiante del terrorismo y sus graves implicaciones para la seguridad nacional de los Estados Miembros.

El debate abordó las amenazas globales asociadas a las herramientas basadas en IA, como la creación y divulgación de desinformación, propaganda y falsificaciones hiperrealistas, que se usan cada vez más como vías de captación y radicalización. Se planteó la preocupación por la automatización de los ataques mediante drones y sistemas autónomos con IA. Se identificaron las vulnerabilidades de ciberseguridad, en especial las que se pueden explotar mediante técnicas de piratería mejoradas con IA y dirigidas a infraestructuras críticas, como un acuciante problema global.

A escala regional, los participantes destacaron las disparidades en cuanto a capacidad tecnológica, que se traducen en distintos niveles de competencia para detectar y contrarrestar las amenazas potenciadas por la IA. Esa desigualdad exacerba los retos asociados a la gestión del riesgo, ya que los algoritmos de los medios sociales a menudo amplifican disputas locales, alimentando la polarización y el extremismo.

También se citaron las implicaciones para la seguridad nacional de estas amenazas y el aumento de los riesgos para las infraestructuras críticas como las redes eléctricas, los sistemas financieros y las comunicaciones. Se estableció que uno de los retos fundamentales para la detección y mitigación de estas amenazas es la sofisticación de las tácticas evasivas mejoradas con IA.

Entre las cuestiones clave abordadas se contaron las siguientes:

- **La naturaleza dual de la IA**: La IA implica tanto oportunidades como riesgos, que requieren una adecuada regulación gubernamental.
- **El rápido crecimiento tecnológico**: El crecimiento exponencial de estas tecnologías suele ir por delante de las medidas regulatorias, lo que provoca déficits en la supervisión.
- **El uso de la IA como arma**: Las organizaciones terroristas están aprovechando la IA para producir y desplegar drones armados y difundir falsificaciones hiperrealistas en zonas de

conflicto. También se han identificado otros riesgos emergentes, como la alteración deliberada de los sistemas de IA con datos corruptos (por ejemplo, ataques de "poisoning" contra grandes modelos lingüísticos).

- **El aprovechamiento para fines de propaganda y captación**: Las organizaciones terroristas utilizan cada vez más la IA para mejorar sus métodos propagandísticos y de captación, y se están registrando avances importantes en el uso de las nuevas tecnologías para fines maliciosos.

SESIÓN II. Buenas prácticas parlamentarias regionales e internacionales para la prevención y la lucha contra el uso de la IA y otras nuevas tecnologías con fines terroristas

La sesión se centró en presentar las prácticas parlamentarias regionales e internacionales que resultan eficaces en la prevención y la lucha contra el uso de la IA y otras nuevas tecnologías con fines terroristas. Entre sus objetivos también se contó la identificación de las estrategias necesarias para poner en marcha medidas eficaces sin comprometer el avance tecnológico y el desarrollo económico. Además, se estudiaron las posibles contribuciones de los parlamentarios y las asambleas parlamentarias a este esfuerzo a escala nacional e internacional.

La sesión incluyó una presentación de la Agencia Nacional de Ciberseguridad italiana (ANC), que gestiona temas de terrorismo como parte de su mandato de seguridad cibernética. La ANC trabaja con los retos derivados de la IA en el marco de la ciberseguridad y le da prioridad a evitar los errores cometidos durante las primeras fases del desarrollo de Internet. Actualmente, la agencia enfatiza la importancia de priorizar la seguridad en las tecnologías emergentes para reducir las vulnerabilidades. Además, pretende mejorar la cooperación entre agencias para diseñar respuestas eficaces a unos retos en constante evolución. Partiendo del reconocimiento del inmenso potencial de estos rápidos avances tecnológicos para producir tanto beneficios como daños, la ANC se está dedicando a predecir su desarrollo para minimizar sus posibles riesgos de seguridad.

La resolución de la AP de la OSCE sobre "Inteligencia artificial y la lucha contra el terrorismo" (aprobada el 29 de junio de 2024, en Bucarest, Rumania) fue uno de los principales temas de debate y se reconoció como una de las mejores prácticas internacionales. La resolución plantea un exhaustivo marco para gestionar las oportunidades y los riesgos derivados de la IA en la lucha contra el terrorismo. Enfatiza la necesidad de combatir el terrorismo y el extremismo violento al tiempo que se defienden los derechos humanos, las libertades fundamentales y el estado de derecho. Tras reconocer el potencial de la IA para incrementar la seguridad, la resolución aborda los riesgos derivados de su uso indebido por parte de organizaciones terroristas para actividades como la planificación, la captación y la difusión de propaganda. La resolución reclama marcos jurídicos y mecanismos de supervisión más sólidos para regular el desarrollo y el uso de la IA, garantizar la transparencia, el cumplimiento ético y la rendición de cuentas. Destaca la importancia de las colaboraciones público-privadas para imponer normas de transparencia y mitigar los riesgos,

así como de la promoción del uso de herramientas de IA para detectar actividades terroristas y luchar contra ellas. Con el fin de impulsar la resiliencia de la sociedad, la resolución aboga por poner en marcha campañas de educación pública, sobre todo destinadas a la juventud, que mejoren la alfabetización mediática y contrarresten la polarización en línea. Además, destaca la importancia del etiquetado obligatorio del contenido generado por IA para combatir la información errónea. La cooperación internacional se presenta como un elemento crítico, por lo que la resolución anima a los Estados a compartir buenas prácticas y conocimientos técnicos a través de foros multilaterales como la OSCE. Con el uso responsable y colaborativo de la IA, la resolución ofrece un enfoque equilibrado para reforzar las iniciativas mundiales de lucha contra el terrorismo a la vez que se salvaguardan los derechos humanos.

El Centre for Global Studies (CGS) de la Asamblea Parlamentaria del Mediterráneo (APM) presentó su reciente informe "El uso malicioso de la IA y las tecnologías emergentes por parte de los grupos terroristas y delictivos: Repercusión en la seguridad, la legislación y la gobernanza". Este informe estudia el uso que hacen de las tecnologías nuevas y emergentes los grupos terroristas, las redes delictivas transnacionales y otros actores no estatales. Valora los efectos de estas tecnologías en la seguridad nacional y regional, así como sus consecuencias para los procesos y las instituciones estatales, incluidos ciberataques, información errónea, desinformación, violencia política, culturas del odio y resiliencia sistémica. Por otra parte, el documento evalúa la situación actual de los marcos normativos relacionados con la seguridad a nivel nacional y continental, destacando áreas en las que hay que mejorar. Es coherente con las directrices estratégicas derivadas de las resoluciones, declaraciones e informes de las Naciones Unidad y sus organizaciones afiliadas, además de con las leyes e iniciativas de gobernanza de la IA de los Estados Miembros de todo el mundo. El informe ofrece un detallado conjunto de recomendaciones estratégicas, técnicas y políticas, muchas de las cuales ponen de manifiesta la función esencial de las respuestas parlamentarias. Como "documento vivo", el objetivo es revisarlo y actualizarlo permanentemente para reflejar la evolución de los retos y las oportunidades.

Como parte de su contribución a las buenas prácticas parlamentarias regionales e internacionales, la Asamblea Interparlamentaria de Naciones Miembros de la Comunidad de Estados Independientes (AIP CEI) aportó un resumen de sus actividades en este ámbito. En 2023, aprobó unas recomendaciones sobre el marco regulatorio de la IA, incluidas directrices éticas de investigación y desarrollo, con el fin de establecer un sistema unificado de normas jurídicas y éticas que promuevan el desarrollo de la IA en los distintos sectores económicos de los Estados Miembros de la CEI, garantizando la protección de los derechos de la ciudadanía y preservando la seguridad. Actualmente, la AIP CEI está redactando una ley modelo, *Sobre las tecnologías de la inteligencia artificial*, para regular todo el ciclo de vida de la IA en consonancia con las agendas de la Asamblea General de las Naciones Unidas y de la Unión Internacional de Telecomunicaciones. Una de las características clave de esta iniciativa es la integración de las evaluaciones de impacto tecnológico en el proceso legislativo para minimizar riesgos y evitar consecuencias negativas para la humanidad. En la misma línea, la AIP CEI está trabajando en otra ley modelo, *Sobre la lucha contra el uso de sistemas autónomos y robóticos para fines terroristas*

y extremistas, que reconoce la necesidad de abordar los retos de seguridad que plantea la rápida evolución de la IA. En un contexto en el que los sistemas autónomos y robóticos se han convertido en dispositivos domésticos habituales, este proyecto legislativo pretende hacer frente a los propósitos delictivos, ya sea de los desarrolladores de sistemas, que son normalmente los responsables del diseño del software, o de los usuarios que intentan utilizar sistemas de uso general para fines maliciosos.

Los expertos y participantes también debatieron la Resolución del Parlamento Europeo sobre la inteligencia artificial en la era digital (aprobada el 3 de mayo de 2022), que es uno de los instrumentos legales más completos en lo referido a la evaluación y la gestión del impacto transformador de la IA y sus implicaciones para el terrorismo, el extremismo y la seguridad. La resolución subraya el papel fundamental de la IA como ayuda para las fuerzas del orden público en la lucha contra la delincuencia organizada, el terrorismo y la ciberdelincuencia. Identifica sectores de alto riesgo como prioritarios en la evaluación de riesgos con el fin de mitigar amenazas potenciales para seguridad si los derechos fundamentales. Dado que el uso indebido de la IA en una guerra híbrida y la injerencia extranjera constituyen preocupaciones de gran calado, la resolución enfatiza riesgos como las campañas de desinformación, la desestabilización económica y la manipulación de elecciones que podrían favorecer a grupos extremistas o socavar instituciones democráticas. También advierte sobre la proliferación de falsificaciones hiperrealistas y robos de identidad facilitados por la IA, que menoscaban la confianza en el contenido digital y exacerban la polarización sociopolítica. La resolución reitera el llamamiento del Parlamento Europeo para prohibir a escala internacional los sistemas de armas autónomos letales (SAAL) y subraya la necesidad de una adecuada supervisión humana de las aplicaciones militares de la IA para garantizar el cumplimiento de los principios jurídicos y éticos. Para resolver estos retos, la resolución pone sobre la mesa la necesidad de marcos regulatorios robustos, flexibles y orientados al futuro que protejan los derechos fundamentales y los derechos humanos.

Los participantes también comentaron la resolución de la Unión Interparlamentaria (UIP) titulada "La repercusión de la inteligencia artificial en la democracia, los derechos humanos y el estado de derecho" aprobada el 17 de octubre de 2024, refiriéndose a su pertinencia en el contexto de la lucha contra el terrorismo. La resolución pone de relieve la importancia del papel activo de los parlamentos en la conformación de las normas de gobernanza de la IA para garantizar que los avances tecnológicos no erosionan los valores democráticos, los derechos humanos y el estado de derecho. Aunque no se ocupa directamente del terrorismo, plantea preocupaciones esenciales, como el potencial de la IA para facilitar la difusión de información errónea, desinformación e ideas extremistas, que pueden desestabilizar sociedades y alimentar ideologías violentas. La resolución enfatiza además el riesgo de que la IA amplifique los sesgos y la discriminación, lo que incluye la violencia de género y el extremismo en línea, y reclama sólidos marcos legales para asegurar la transparencia y la rendición de cuentas en el desarrollo y el despliegue de la IA. Además, la resolución aboga por que la gobernanza de la IA asuma un enfoque centrado en el ser humano, urgiendo a tomar medidas para evitar el uso indebido de la IA para la vigilancia, la manipulación de datos y la creación de contenido dañino, como las falsificaciones hiperrealistas generadas con IA. Subraya la necesidad de cooperación internacional inclusiva para asegurar que las tecnologías

de IA se usan de forma responsable y equitativa, protegiendo los derechos individuales y fomentando la confianza social. Además, la resolución insta a los parlamentos a priorizar la educación y la capacitación en materia de IA, garantizando la disponibilidad de habilidades para abordar los retos que plantean las tecnologías emergentes, incluida su potencial repercusión en la seguridad nacional y la lucha contra el terrorismo.

Durante el diálogo se citó la "Convención marco del Consejo de Europa sobre inteligencia artificial y derechos humanos, democracia y estado de derecho", así como otros instrumentos internacionales. Aunque no trata explícitamente cuestiones relacionadas con el terrorismo, es el primer tratado internacional legalmente vinculante sobre la IA en centrarse específicamente en los derechos humanos, la democracia y el estado de derecho. El objetivo de la Convención es garantizar que todas las actividades que conforman el ciclo de vida de los sistemas de inteligencia artificial respetan plenamente los derechos humanos, la democracia y el estado de derecho, al tiempo que se promueve la innovación y el avance tecnológico. Además, pretende subsanar cualquier laguna jurídica que pueda derivarse del rápido desarrollo de la tecnología.

SESIÓN III. El marco jurídico internacional para la prevención y la lucha contra el uso de la IA y otras nuevas tecnologías con fines terroristas

La tercera sesión, que se basó en los debates anteriores sobre los retos, las amenazas y las prácticas vigentes, se centró fundamentalmente en el trabajo y las recomendaciones de las entidades correspondientes de las Naciones Unidas, así como de las organizaciones internacionales y regionales, para la prevención y la lucha contra el uso de la IA y otras nuevas tecnologías con fines terroristas. La sesión también abordó el apoyo que estas organizaciones pueden prestar a los Estados Miembros, incluidos sus órganos legislativos, para la aplicación de las resoluciones y las recomendaciones del Consejo de Seguridad de las Naciones Unidas en materia de IA y nuevas tecnologías.

La Dependencia de Ciberseguridad y Nuevas Tecnologías de la Oficina de las Naciones Unidas de Lucha Contra el Terrorismo / Centro de las Naciones Unidas contra el Terrorismo (OLCT/CNUCT) presentó sus actividades de refuerzo de las competencias de las fuerzas del orden público y los sistemas de justicia penal en los países asociados seleccionados para luchar contra el uso de las nuevas tecnologías y de las tecnologías emergentes con fines terroristas. La Dependencia también destacó su labor de apoyo a los Estados Miembros en el aprovechamiento de estas tecnologías para poner fin al terrorismo. Además, la Dependencia mostró su serie de publicaciones sobre ciberseguridad y nuevas tecnologías, que incluyen:

- *La evaluación de amenazas terroristas: El uso de las nuevas tecnologías con fines terroristas;*
- *El diseño de respuestas políticas nacionales de lucha contra el terrorismo para impedir el uso de las nuevas tecnologías con fines terroristas;*
- *Marco de capacidades de aplicación jurídica para las nuevas tecnologías en la lucha contra el terrorismo;*

- *La lucha contra el terrorismo en línea con inteligencia artificial: Una panorámica de las agencias de lucha contra el terrorismo y aplicación de la ley en Asia Meridional y el Sudeste Asiático;*
- *Algoritmos y terrorismo: El uso malicioso de la inteligencia artificial con fines terroristas*.

La Unidad de Acción contra el Terrorismo de la Organización para la Seguridad y la Cooperación en Europa (OSCE) expuso sus perspectivas y experiencias en la prevención y la lucha contra el uso de la IA y las nuevas tecnologías con fines terroristas. La Unidad enfatizó que su labor se alinea con la resolución aprobada recientemente por la OSCE en materia de IA y lucha contra el terrorismo. Subrayó la importancia de implicar a un amplio abanico de actores no gubernamentales —como la sociedad civil, las mujeres, la juventud, las empresas, la industria y los medios de comunicación— en la prevención del extremismo violento y de la radicalización conducente al terrorismo (EVRCT). La presentación también incidió en que es fundamental respaldar a estos actores para que puedan usar la IA para resolver los retos relacionados con la prevención del EVRCT, siempre valorando rigurosamente sus implicaciones éticas, mitigando los sesgos algorítmicos y preservando los derechos humanos y la privacidad.

La Subdivisión de Prevención del Terrorismo de la Oficina de las Naciones Unidas contra la Droga y el Delito (SPT UNODC) habló sobre su trabajo de promoción del uso ético y responsable de la IA y las tecnologías avanzadas para prevenir y contrarrestar el uso indebido de los espacios virtuales por parte de los terroristas. Su intervención puso de manifiesto que los grupos terroristas y extremistas violentos están recurriendo cada vez más al ámbito digital para actividades como la difusión de propaganda, la incitación, la captación y la coordinación operativa. La SPT UNODC citó investigaciones que indican que estos grupos están experimentando con herramientas de IA generativa para mejorar sus estrategias propagandísticas. Eso incluye probar capacidades como la generación de contenido multimedia, las traducciones multilingües automatizadas, la creación de propaganda sintética, el reciclaje de variantes, los mensajes personalizados y el uso de métodos para sortear los sistemas de moderación y ampliar su alcance. Por otra parte, la UNODC incidió en la reciente aprobación de la Convención de las Naciones Unidas contra la Ciberdelincuencia, en la que actuó como Secretaría. Este innovador tratado de carácter mundial ofrece a los países medidas esenciales para prevenir y combatir la ciber delincuencia, además de promover una mayor cooperación internacional en el intercambio de pruebas electrónicas para procedimientos penales graves.

En su intervención, el Comité contra el Terrorismo (CT) del Consejo de Seguridad y la Dirección Ejecutiva del Comité contra el Terrorismo (DECT) destacaron el apoyo de la DECT a los Estados Miembros en la identificación de enfoques innovadores y colaborativos para luchar contra el uso indebido de las TIC por parte de los terroristas. La presentación enfatizó el desarrollo de soluciones tecnológicas que aprovechen todo el potencial de las TIC para fines positivos desde el respeto a los derechos humanos, las libertades fundamentales y las obligaciones jurídicas internacionales. La DECT también habló de promover y facilitar asistencia técnica y de impulsar las colaboraciones público-privadas para luchar contra la apropiación de los grupos terroristas de las tecnologías digitales. Además, la DECT ayuda a los Estados Miembros a contrarrestar las narrativas terroristas

tanto en línea como en el mundo físico, subrayando la importancia de encontrar un enfoque equilibrado que luche contra los discursos del odio sin comprometer la libertad de expresión. La presentación incidió en la necesidad de que los Estados colaboren en el desarrollo de soluciones sostenibles a estos retos y en que resulta fundamental encontrar una base común compartida a pesar de las diferencias. La DECT formuló recomendaciones esenciales sobre medidas para prevenir y luchar contra el uso de la IA y las tecnologías emergentes con fines terroristas. Entre estas recomendaciones se contaron la capacitación de los sistemas de justicia penal para resolver los delitos relacionados con la IA y las TIC y la mejora de la rendición de cuentas mediante mecanismos que garanticen que las empresas asumen responsabilidades por las prácticas que permiten un uso indebido de sus plataformas —por ejemplo, algoritmos nocivos, espacios no moderados o venta de servicios a grupos terroristas— y el desarrollo de una "norma técnica mínima" mundial para que los gobiernos puedan prevenir y combatir eficazmente el terrorismo basado en las TIC.

RECOMENDACIONES

Los expertos y participantes en el diálogo plantearon las siguientes recomendaciones, convenientemente estructuradas en siete áreas temáticas, para abordar las oportunidades y los retos derivados de la IA y las tecnologías emergentes en la lucha contra el terrorismo.

1. Desarrollo político y legislativo
• Desarrollar una sólida legislación nacional para regular el uso de la IA y las tecnologías emergentes, garantizando que aborda las preocupaciones referentes a su dualidad (aplicaciones tanto beneficiosas como dañinas) con el fin de evitar el uso indebido por parte de grupos terroristas. • Promulgar nuevas leyes y actualizar las existentes para penar explícitamente el uso indebido de la IA y las nuevas tecnologías para fines delictivos, incluido el terrorismo. • Armonizar la legislación sobre IA y tecnologías emergentes en todos los países para garantizar su coherencia. • Establecer normas comunes para la ciencia forense digital y las pruebas electrónicas. • Garantizar que la legislación y las normativas están cuidadosamente equilibradas para evitar la sobrerregulación, que podría obstaculizar el desarrollo y el avance tecnológico. Dada la rapidez con la que evolucionan estas tecnologías, la legislación debe ser flexible y adaptable, ya que los marcos jurídicos tradicionales suelen tener problemas para seguir el ritmo de la innovación. Este equilibrio debe alcanzarse mediante la cooperación mundial y el respeto de los derechos fundamentales.
2. Derechos humanos y protección de datos
• Garantizar que las medidas de lucha contra el terrorismo cumplen los derechos humanos, priorizando la protección de los datos personales y la defensa de la justicia, la igualdad y la equidad.

- Poner en marcha medidas eficaces para salvaguardar los datos y la información personal a través de mecanismos acordes a los derechos humanos.
- Tener en cuenta las implicaciones éticas, los sesgos algorítmicos y las cuestiones fundamentales de privacidad cuando se use la IA en la lucha contra el terrorismo.

3. Desarrollo de capacidades para los sistemas judiciales y de orden público

- Equipar y formar a las fuerzas del orden público para luchar eficazmente contra las actividades terroristas y extremistas basadas en IA, garantizando el respeto de las normas internacionales sobre derechos humanos.
- Mejorar la capacitación de los sistemas de justicia penal para resolver los delitos relacionados con la IA y las TIC.
- Ofrecer recursos y formación exhaustiva para preparar a las fuerzas del orden público ante los retos que plantean las tecnologías emergentes.

4. Educación y concienciación pública

- Priorizar las inversiones en educación y alfabetización digital con el fin de capacitar a la ciudadanía, especialmente a la juventud, para hacer un análisis crítico de la información, reconocer la información errónea y combatir la propaganda extremista.
- Integrar la IA y las tecnologías emergentes en los planes de estudios para ayudar a los individuos a identificar el contenido extremista y entender sus riesgos.
- Apoyar las iniciativas educativas públicas destinadas al fomento de la resiliencia frente a las campañas de desinformación y propaganda vehiculadas mediante IA.
- Promover las iniciativas de concienciación pública, inclusive la alfabetización mediática y el etiquetado del contenido generado mediante IA, para combatir la información errónea.

5. Colaboraciones y cooperación internacional

- Incrementar la cooperación internacional para abordar el uso transnacional de la IA y las nuevas tecnologías con fines maliciosos, fomentando la colaboración transfronteriza.
- Apoyar la creación de una agencia de seguridad internacional, una "CiberPol" basada en el modelo de la Interpol, para luchar contra la ciber delincuencia y el terrorismo a escala mundial.
- Facilitar la cooperación entre las autoridades nacionales, los órganos regionales y las organizaciones internacionales para compartir datos de inteligencia, buenas prácticas y conocimientos tecnológicos.
- Impulsar la cooperación multilateral y las colaboraciones público-privadas para promover la transparencia y la rendición de cuentas en la labor de lucha contra el terrorismo.

• Incentivar la colaboración transfronteriza con el fin de garantizar la eficacia y la coherencia de las actividades de lucha contra el terrorismo y el extremismo violento.
6. Colaboración con el sector tecnológico
• Promover una estrecha colaboración entre los gobiernos, el sector de las TIC y la industria tecnológica para crear salvaguardas que eviten el uso indebido de la IA por parte de organizaciones terroristas. • Mejorar la rendición de cuentas en el sector tecnológico, garantizando que las empresas asumen su responsabilidad por prácticas que permiten el uso indebido, como, por ejemplo, los algoritmos nocivos, los espacios no moderados o la venta de servicios a grupos terroristas. • Desarrollar una "norma técnica mínima" mundial para que los gobiernos puedan prevenir y combatir eficazmente el terrorismo basado en las TIC. • Incentivar la colaboración con las empresas tecnológicas para mejorar la detección de amenazas y mitigar los riesgos asociados a las plataformas y herramientas de IA.
7. Función de las asambleas parlamentarias
• Aprovechar las asambleas parlamentarias para concienciar, promover la creación de normas internacionales y abogar por la disponibilidad de asistencia técnica para las medidas de lucha contra el terrorismo. • Los parlamentarios deben liderar las iniciativas para facilitar y promover la colaboración internacional en la lucha contra el terrorismo a todos los niveles, garantizando que las estrategias nacionales son coherentes con las normas internacionales.

CONCLUSIÓN Y MEDIDAS DE SEGUIMIENTO

Los debates de los expertos y las contribuciones de los participantes durante el diálogo pusieron de manifiesto la naturaleza cambiante de los desafíos que la IA y las tecnologías emergentes plantean en la lucha contra el terrorismo. Las principales recomendaciones formuladas se refieren a varios ámbitos fundamentales, incluidos el desarrollo legislativo, la protección de los derechos humanos, la capacitación de las fuerzas del orden público, la educación pública, la colaboración internacional y la función de las asambleas parlamentarias. El objetivo de estas recomendaciones es asegurar una respuesta equilibrada, coordinada y acorde a los derechos humanos a las oportunidades y riesgos que presentan estas tecnologías en la prevención y la lucha contra el terrorismo y el extremismo violento.

Para avanzar en la aplicación de estas recomendaciones, la Oficina del Programa de la OLCT sobre la Colaboración Parlamentaria en la prevención y la lucha contra el terrorismo continuará facilitando la colaboración entre los órganos parlamentarios, los gobiernos nacionales, las agencias de las Naciones Unidas y otras partes interesadas. Esta coordinación permanente respaldará el

desarrollo de estrategias y políticas que integren la IA y las tecnologías emergentes en las iniciativas de lucha contra el terrorismo y PEV (prevención del extremismo violento), concediendo prioridad al desarrollo de capacidades y la asistencia técnica.

Con la vista puesta en el periodo 2025-2026, la Oficina del Programa sobre la Colaboración Parlamentaria, en colaboración con la Dependencia de Ciberseguridad y Nuevas Tecnologías de la OLCT/CNUCT, organizará una conferencia parlamentaria mundial sobre IA y tecnologías emergentes. La finalidad de la conferencia será servir de plataforma para el diálogo parlamentario, centrando el debate en las respuestas eficaces a la intersección de la IA, las nuevas tecnologías y la lucha contra el terrorismo.

Además, la OLCT se fijará la meta de organizar una serie de actividades de concienciación y capacitación para los parlamentarios y para todo el personal pertinente de los parlamentos nacionales y las asambleas parlamentarias. El objetivo de estas actividades será mejorar su comprensión sobre la IA y las nuevas tecnologías en el contexto de la LCT/PEV, lo que les permitirá tomar decisiones más fundamentadas y respetuosas con los derechos humanos en el marco de su labor política y legislativa.

Las asambleas parlamentarias asociadas, en especial las participantes en el Mecanismo de Coordinación de las Asambleas Parlamentarias para la Lucha contra el Terrorismo, tendrán un papel fundamental para la puesta en práctica de estas iniciativas. La OLCT colaborará estrechamente con estas asambleas para ofrecer asesoramiento, apoyo y conocimientos adaptados a los parlamentos nacionales, garantizando su implicación activa en el impulso de la lucha contra el terrorismo.

Por último, se priorizará la divulgación de las recomendaciones de los expertos para garantizar que todos los socios, las partes interesadas y asambleas parlamentarias pertinentes adaptamos sus iniciativas, fomentando una respuesta mundial coordinada a los retos que plantean las tecnologías emergentes en la lucha contra el terrorismo.

El siguiente (quinto) Diálogo Parlamentario sobre Políticas está previsto para el segundo trimestre de 2025; la fecha, el lugar y el tema están todavía por confirmar.

COMUNICACIÓN

Comunicados de prensa

https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/20241205_press_release_4th_policy_dialogue_rome.pdf

https://www.oscepa.org/en/news-a-media/press-releases/press-2024/under-osce-pa-leadership-legislators-from-across-the-globe-discuss-preventing-and-countering-the-use-of-ai-by-terrorists-at-policy-dialogue-in-rome

https://www.shura.qa/en/Pages/MediaCenter/News/07122024

https://pam.int/the-fourth-parliamentary-policy-dialogue/

https://turkpa.org/news/1766-turkpa-attended-6th-meeting-of-coordination-mechanism-for-parliamentary-assemblies-on-counter-terrorism-and-4th-parliamentary-policy-dialogue-organized-by-unoct

https://italyun.esteri.it/en/news/dalla_rappresentanza/2024/12/closing-remarks-delivered-by-permanent-representative-amb-maurizio-massari-at-fourth-parliamentary-policy-dialogue-on-countering-the-use-of-artificial-intelligence-and-new-technologies-for-terrorist/

Tuits:

https://x.com/UN_OCT/status/1865127801377927552

https://x.com/oscepa/status/1864327102989734107