Naciones Unidas A/HRC/52/39

Asamblea General

Distr. general
1 de marzo de 2023
Español
Original: inglés

Consejo de Derechos Humanos
52º período de sesiones
27 de febrero a 31 de marzo de 2023
Tema 3 de la agenda
Promoción y protección de todos los derechos humanos, civiles, políticos, económicos, sociales y culturales, incluido el derecho al desarrollo

Repercusiones en los derechos humanos del desarrollo, el uso y la transferencia de nuevas tecnologías en el contexto de la lucha contra el terrorismo y la prevención y represión del extremismo violento

Informe de la Relatora Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, Fionnuala Ní Aoláin* **

Resumen

En el presente informe, la Relatora Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, Fionnuala Ní Aoláin, expone los retos y las consecuencias que entrañan para los derechos humanos el desarrollo, el uso y la transferencia de nuevas tecnologías en el contexto de la lucha contra el terrorismo y el extremismo violento. La Relatora Especial reconoce la capacidad que tienen las nuevas tecnologías para transformar positivamente las vidas y fomentar la plena efectividad de los derechos humanos, la igualdad y la dignidad de los seres humanos, así como el importante potencial que ofrecen las nuevas tecnologías para colmar las lagunas existentes en materia de derechos humanos de las personas más marginadas y vulnerables. Lamentablemente, al mismo tiempo, las nuevas tecnologías se están utilizando indebidamente en todo el mundo para restringir y violar los derechos humanos.

En el presente informe se ilustran las formas en que la lucha contra el terrorismo y la seguridad se utilizan habitualmente para proporcionar argumentos políticos y jurídicos que justifiquen la adopción de tecnologías de alto riesgo y sumamente intrusivas sobre la base de amenazas excepcionales y bajo la promesa de una aplicación estrictamente limitada. En el informe se demuestra además que tales justificaciones y limitaciones rara vez son válidas y que el argumento del uso excepcional para responder a crisis de seguridad es una quimera, ya que, en la realidad, se hace un uso amplio y generalizado de estas tecnologías que carece de las restricciones adecuadas en materia de derechos

* Este informe se ha presentado fuera de plazo para reflejar en él las novedades más recientes.
** El anexo del presente informe se distribuye tal como se recibió, únicamente en el idioma en que fue presentado.

humanos o estado de derecho. Estas tecnologías, como la biométrica, la de vigilancia y la de los drones, tienen graves repercusiones en el disfrute de los derechos humanos a nivel mundial. La Relatora Especial destaca los riesgos para los derechos humanos que entrañan el desarrollo, el despliegue y la transferencia de esas tecnologías a escala internacional. Asimismo, le preocupan profundamente los elementos discriminatorios que conlleva el desarrollo y el despliegue de dichas tecnologías. Algunas de las consecuencias negativas son las violaciones directas de los derechos inderogables —cuya integridad está siendo socavada por nuevas tecnologías que carecen de cualquier supervisión legal significativa— y la impunidad de los agentes tanto estatales como no estatales, que, al utilizar y transferir dichas tecnologías, incurren en prácticas que violan sistemáticamente los derechos. Las repercusiones en los derechos humanos a nivel mundial son devastadoras, especialmente en el ejercicio de los derechos a la privacidad, la expresión, la asociación y la participación política. La cuestión principal que plantea la Relatora Especial es que las prácticas abusivas están muy arraigadas en el ámbito de la lucha contra el terrorismo y el extremismo violento, precisamente porque, a falta de una definición de esos fenómenos acordada internacionalmente, cada Estado los define para promover determinados intereses, pocos de los cuales están relacionados con los derechos humanos y el estado de derecho. La Relatora Especial pide una moratoria sobre el uso de determinadas tecnologías, incluida una prohibición a nivel mundial de los sistemas de armas autónomos letales. En concreto, insta a los Estados Miembros a que adopten una política de cese y desistimiento con respecto a la transferencia de esas tecnologías a Estados que tengan un historial demostrado de violaciones de los derechos humanos, según confirman las resoluciones del Consejo de Derechos Humanos y de la Asamblea General y las conclusiones de los órganos de las Naciones Unidas creados en virtud de tratados de derechos humanos. Haciéndose eco del llamamiento del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, pide que se imponga una moratoria a la transferencia de tecnologías de vigilancia. Asimismo, presenta un modelo para la creación de un marco normativo mundial sobre el uso de las tecnologías de vigilancia.

I. Actividades de la Relatora Especial

1. La Relatora Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, Fionnuala Ní Aoláin, presentó a la Asamblea General en octubre de 2022 su informe sobre el efecto de la lucha contra el terrorismo en el establecimiento, la consolidación y el sostenimiento de la paz y en la prevención y la solución de conflictos[1].

2. La Relatora Especial sigue priorizando la colaboración positiva y estrecha con los Estados Miembros a nivel nacional. Realizó visitas constructivas a Maldivas (15 a 24 de mayo de 2022)[2] y a Bosnia y Herzegovina (13 a 20 de enero de 2023)[3]. Realizó una visita formativa de ámbito operacional a la Misión Multidimensional Integrada de Estabilización de las Naciones Unidas en Malí en julio de 2022. En marzo de 2022, tras la publicación de su informe de seguimiento del estudio conjunto de 2010 sobre las prácticas mundiales en relación con la detención secreta en el contexto de la lucha contra el terrorismo[4], el Gobierno de los Estados Unidos de América cursó una invitación preliminar para debatir una posible visita técnica dedicada al centro de detención de la bahía de Guantánamo (Cuba), al reasentamiento/repatriación de antiguos detenidos y a los derechos humanos de las víctimas de los sucesos del 11 de septiembre de 2001 y de sus familiares. Tras extensos y constructivos debates, la visita al centro de detención tuvo lugar del 6 al 10 de febrero de 2023, mientras que los demás aspectos de la visita se concretarán hasta abril de 2023. Una vez finalizada la visita técnica se emitirá una declaración de fin de misión.

3. La Relatora Especial ha mantenido su compromiso de colaborar activamente con diversos agentes de la sociedad civil, logrando así una plena integración en su trabajo de las experiencias sobre el terreno de las prácticas de seguridad y lucha contra el terrorismo. El 9 de mayo de 2022, antes de la Conferencia Internacional de Alto Nivel sobre Derechos Humanos, Sociedad Civil y Lucha contra el Terrorismo, la Relatora Especial y España coorganizaron un taller de la sociedad civil en Málaga. Representantes de la sociedad civil de 43 países participaron en una serie de consultas para elaborar un documento final que se incluirá en el resultado oficial de la conferencia. Además, la Relatora Especial puso en marcha un estudio global sobre las repercusiones de las medidas antiterroristas en la sociedad civil y el espacio cívico, con el apoyo de Alemania y España, y realizó una serie de cortometrajes que documentan las consecuencias que las medidas antiterroristas tienen para los agentes de la sociedad civil en todo el mundo.

4. La Relatora Especial considera prioritario proporcionar a los Estados asistencia técnica y opiniones sobre la legislación de lucha contra el terrorismo. Desde 2021, ha realizado exámenes de la legislación o de la evolución legislativa de Argelia, Austria, Belarús, el Brasil, China, Dinamarca, El Salvador, Francia, Haití, Malí, Nicaragua, Nueva Zelandia, el Reino de los Países Bajos, el Reino Unido de Gran Bretaña e Irlanda del Norte, Sri Lanka, Tailandia, Tayikistán, Türkiye, Uzbekistán, Venezuela (República Bolivariana de) y Zimbabwe, así como de la Unión Europea.

5. La Relatora Especial publicó documentos de posición sobre las repercusiones de las sanciones antiterroristas en las obligaciones de los Estados en materia de derechos humanos y derecho internacional, haciendo especial referencia a los regímenes de sanciones previstos en las resoluciones del Consejo de Seguridad 1267 (1999) y 1988 (2011)[5]; sobre las consecuencias para los derechos humanos de la privación de la ciudadanía en el contexto de la lucha contra el terrorismo, refiriéndose específicamente a la situación en el noreste de la República Árabe Siria[6]; sobre las consecuencias para los derechos humanos y el estado de

[1] A/77/345.

[2] Véanse A/HRC/52/39/Add.1 y Add.2.

[3] Véase https://www.ohchr.org/en/press-releases/2023/01/bosnia-and-herzegovina-divisive-post-conflict-politics-and-failure-address.

[4] A/HRC/49/45.

[5] Véase https://www.ohchr.org/sites/default/files/2022-03/position-paper-unsrct-on-unsc-use-of-ct-targeted-sanctions.pdf.

[6] Véase https://www.ohchr.org/es/special-procedures/sr-terrorism/return-and-repatriation-foreign-fighters-and-their-families.

derecho de las medidas de lucha contra la financiación del terrorismo[7]; sobre la regulación del comercio internacional de tecnologías de programas espía para la lucha contra el terrorismo[8]; y sobre el uso de drones armados[9].

6. La Relatora Especial sigue formando parte del Equipo Especial del Pacto Mundial de Coordinación de la Lucha Antiterrorista de las Naciones Unidas y está profundamente comprometida con el enfoque de toda la Organización de las Naciones Unidas para luchar contra el terrorismo, en el que se integran los derechos humanos tal y como se afirma en la Estrategia Global de las Naciones Unidas contra el Terrorismo. Mantiene una cooperación positiva con el Grupo de Acción Financiera. Ha participado en tres reuniones del Comité Interamericano contra el Terrorismo. En el último año ha realizado varias reuniones informativas para grupos regionales, entre ellos la Organización de Cooperación Islámica, la Unión Africana, la Unión Europea y el Grupo de América Latina y el Caribe, y se unió al Comité contra el Terrorismo para su período extraordinario de sesiones en Mumbai y Nueva Delhi (India).

II. Desarrollo, uso y transferencia de nuevas tecnologías en el contexto de la lucha contra el terrorismo y la prevención y represión del extremismo violento

7. Es indiscutible que las nuevas tecnologías pueden ofrecer enormes beneficios, pues propician y promueven la dignidad humana, favorecen el desarrollo sostenible y niveles de vida más elevados, contribuyen a mejorar la atención sanitaria, refuerzan la conexión y la comunicación, fomentan la creación de nuevas modalidades educativas y el acceso a ellas, y aumentan la seguridad y la eficiencia de las comunidades. Esos beneficios, cuando se distribuyen de forma equitativa, transparente y no discriminatoria, pueden hacer de la tecnología un aliado en la promoción y protección de los derechos civiles, políticos, económicos, sociales y culturales de los pueblos de todo el planeta.

8. Lamentablemente, los efectos positivos que las nuevas tecnologías pueden tener para los derechos humanos están lejos de materializarse. Por el contrario, las nuevas tecnologías, en particular las digitales, están transformando las formas en que se restringen y violan los derechos humanos en todo el mundo. Varios titulares de mandatos de los procedimientos especiales y el Alto Comisionado de las Naciones Unidas para los Derechos Humanos han abordado la cuestión de la intersección entre los derechos humanos y las tecnologías digitales, en particular el uso de estas tecnologías para fomentar el trato xenófobo y racialmente discriminatorio y la exclusión[10]. Reconociendo y reiterando la importancia de la labor realizada anteriormente, en el presente informe la Relatora Especial se centra en la intersección entre, de un lado, la lucha contra el terrorismo y la prevención y represión del extremismo violento y, de otro, el uso de las nuevas tecnologías. Asimismo, tiene debidamente en cuenta el enfoque estratégico y la hoja de ruta de todo el sistema de las Naciones Unidas para promover el desarrollo de capacidades en materia de inteligencia artificial (IA)[11].

9. La Relatora Especial llama la atención sobre el modo en que los imperativos de seguridad y los argumentos de la lucha contra el terrorismo se utilizan para justificar el desarrollo, el uso y la transferencia de nuevas tecnologías, incluidas, entre otras, las tecnologías biométricas, la IA, las aeronaves no tripuladas (drones) y las herramientas de vigilancia. Denuncia el uso que, bajo el pretexto de prevenir el terrorismo, se ha hecho de algunas nuevas tecnologías que, en la práctica, suponen un profundo menoscabo de los derechos de las personas y las comunidades. Las tecnologías de alto riesgo se han introducido por la proverbial “puerta trasera” y se han legitimado invocando razones de seguridad,

[7] Véase https://www.ohchr.org/sites/default/files/2022-06/2022-06-13-SRCT-HR-CFT-Position-Paper.pdf.

[8] Véase https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/2022-12-15/position-paper-unsrct-on-global-regulation-ct-spyware-technology-trade.pdf.

[9] Véase https://www.ohchr.org/es/special-procedures/sr-terrorism/activities.

[10] Véase A/HRC/48/76.

[11] CEB/2019/1/Add.3.

cuando, en realidad, debilitan la seguridad colectiva global y socavan la promoción y protección de los derechos humanos. Algunos Estados con historiales atroces en materia de derechos humanos, muchos de ellos desprovistos de las más básicas medidas de protección legislativas o judiciales, han recibido carta blanca para acceder a tecnologías de alto riesgo, que han sido utilizadas por esos mismos Estados para reprimir la disidencia legítima, la defensa de los derechos humanos —en particular los de las mujeres y los niños— la representación jurídica, la libertad de expresión en los medios de comunicación y la acción humanitaria.

10. La Relatora Especial reconoce la amenaza que supone el terrorismo para las personas, las comunidades y las sociedades. Es perfectamente consciente del sufrimiento que producen los actos indiscriminados de violencia política dirigidos contra civiles y reafirma su inquebrantable compromiso con las víctimas del terrorismo y con sus familias y comunidades. Sigue instando a los Estados y a las instituciones multilaterales a que afronten y eliminen de manera efectiva las causas interseccionales del terrorismo y de la violencia compleja, incluidos los conflictos armados[12].

11. Sin embargo, la Relatora Especial lamenta la creciente estrechez de miras en el planteamiento de la seguridad que ha venido acompañando a un enfoque particularmente restrictivo de la lucha contra el terrorismo, en particular en el seno de las instituciones multilaterales. El diagnóstico de la amenaza terrorista en los contextos nacionales, así como en los órganos de las Naciones Unidas de lucha contra el terrorismo, se caracteriza por la habitual falta de un enfoque holístico de los factores causales, las formas interseccionales y la producción correlacional de la violencia. En cambio, los encargados de formular políticas optan por tópicos simplistas y manidos sobre las causas de la violencia y proponen respuestas que simplemente no funcionan. La manera actual de luchar contra el terrorismo y el análisis incompleto de sus causas contribuyen a que se produzca un fracaso inaceptable a la hora de combatir de forma efectiva el terrorismo y la violencia compleja en todo el mundo. Las respuestas basadas en análisis causales inadecuados y en datos sesgados, en muchos casos, han exacerbado la violencia en lugar de reducirla. Es en este universo donde se produce la adopción de nuevas tecnologías, a menudo presentadas de forma sensacionalista como la "solución" al fenómeno del terrorismo, que está insuficientemente definido o simplemente no está definido en absoluto. A juicio de la Relatora Especial, la idoneidad, la necesidad y el valor añadido de las nuevas tecnologías deberían someterse a un escrutinio más riguroso antes de ser adoptadas con entusiasmo y sin cuestionamientos en contextos de lucha contra el terrorismo. Es necesario plantearse cuestiones fundamentales sobre si estas tecnologías contribuirán a proteger los derechos humanos, el estado de derecho y la igualdad, o los pondrán en peligro, en un ámbito que se define cada vez más por los atentados contra la dignidad humana.

12. La Relatora Especial destaca tres tendencias en particular que caracterizan el uso de las nuevas tecnologías en la lucha contra el terrorismo y la prevención y represión del extremismo violento. La primera es la instrumentalización del terrorismo para justificar la adopción de tecnologías de alto riesgo, con el pretexto de la excepcionalidad que contamina los debates sobre leyes y políticas. Esto incluye la práctica de introducir excepciones por motivos de seguridad nacional o antiterrorismo en las leyes que regulan las tecnologías emergentes. La segunda concierne a la ausencia de un análisis y una práctica coherentes de los derechos humanos en el desarrollo, el uso y la transferencia de nuevas tecnologías. La referencia superficial y meramente formal a los derechos humanos es una constante en este ámbito. El resultado ha sido un fracaso estrepitoso a la hora de regular las tecnologías de alto riesgo, con consecuencias nefastas a nivel mundial para los derechos humanos y el estado de derecho internacional. La tercera implica la transición, previsible e insidiosa, del uso excepcional inicial de las nuevas tecnologías en contextos de seguridad restringidos al uso generalizado, con la incorporación y normalización de estas tecnologías en la vida cotidiana.

13. En el presente informe, la Relatora Especial presta una atención particular a las transferencias bilaterales y multilaterales de las tecnologías en el ámbito de la lucha contra el terrorismo, y destaca los fallos de los Estados y de las instituciones multilaterales a la hora de establecer sistemas rigurosos de supervisión y control para evitar cualquier uso indebido.

[12] Véase A/77/345.

La aparente falta de voluntad para regular las prácticas de las entidades privadas —incluidas las empresas multinacionales— que violan los derechos humanos es motivo de profunda preocupación. El informe contiene varias recomendaciones específicas y aplicables que se basan en recomendaciones anteriores para aplicar los Principios Rectores sobre las Empresas y los Derechos Humanos (incluido el aprovechamiento del proyecto B-Tech de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (ACNUDH)) y reforzar otros mecanismos creados en virtud de tratados y de regulación de las exportaciones.

14. Lamentablemente, las propias Naciones Unidas parecen dedicarse a apoyar y posibilitar la asistencia técnica y el fomento de la capacidad para la lucha contra el terrorismo en el ámbito de las nuevas tecnologías con una programación que no hace plenamente operativas las obligaciones de diligencia debida relativas a los derechos humanos, además de infravalorar sistemáticamente los riesgos de uso indebido de estas tecnologías. En lo que respecta a las entidades de las Naciones Unidas, la asistencia técnica y el fomento de la capacidad relacionados con tecnologías de alto riesgo —como la IA, la biometría y la ciberseguridad— en contextos de lucha antiterrorista deben llevarse a cabo en consonancia con el derecho internacional de los derechos humanos, el derecho de los refugiados y el derecho humanitario, así como con la política de diligencia debida en materia de derechos humanos. Asimismo, las entidades de las Naciones Unidas deberían guiarse por la estrategia del Secretario General en materia de nuevas tecnologías, cuyo objetivo es definir cómo el sistema de las Naciones Unidas apoyará el uso de estas tecnologías a fin de impulsar la consecución de la Agenda 2030 para el Desarrollo Sostenible y facilitar su armonización con los valores consagrados en la Carta de las Naciones Unidas, la Declaración Universal de Derechos Humanos y las normas y estándares del derecho internacional. En primer lugar, la Relatora Especial apoya los llamamientos a un diálogo sustantivo entre las empresas tecnológicas y de telecomunicaciones, los expertos en derechos humanos de las Naciones Unidas y la sociedad civil, que propicie un enfoque de múltiples interesados sólido en la regulación de estas tecnologías. Este diálogo deberá ajustarse plenamente a las medidas de reglamentación prácticas para incorporar un enfoque basado en los derechos humanos en el desarrollo, el uso y la transferencia de las nuevas tecnologías. En el presente informe se formulan recomendaciones específicas al respecto.

15. La Relatora Especial destaca el papel acelerador que ha desempeñado el Consejo de Seguridad en la integración y legitimación del uso generalizado de las nuevas tecnologías en la lucha antiterrorista mediante las resoluciones aprobadas en virtud del Capítulo VII de la Carta[13]. Coincide con la opinión de que el Consejo debe ejercer sus facultades de regulación en materia de lucha antiterrorista con cautela, discreción y autocontrol y evitar extralimitarse como ha ocurrido con las resoluciones relativas a la lucha antiterrorista desde la 1373 (2001) en adelante[14]. Señala el reciente examen del Comité contra el Terrorismo sobre el uso indebido de drones, tecnologías de la información y las comunicaciones y nuevos métodos de pago y recaudación de fondos en línea por parte de terroristas. En este contexto, la India, en su calidad de Presidente del Comité, promovió un diálogo extenso y constructivo con múltiples partes interesadas y expertos, entre ellos agentes independientes de la sociedad civil. La Relatora Especial encomia este proceso inclusivo, que culminó con la aprobación de la Declaración de Delhi (no vinculante) sobre la lucha contra el uso de las tecnologías nuevas y emergentes con fines terroristas [15], y alienta a la Presidencia entrante, los Emiratos Árabes Unidos, a que adopte un enfoque similar e incorpore la inclusión a la labor ordinaria del Comité. La Declaración representa un avance en el reconocimiento de la importancia de los derechos humanos para la regulación de tecnologías sensibles y de riesgo. No obstante, a la Relatora Especial le preocupa profundamente que la Declaración no contemple el contexto más amplio del uso indebido que hacen los Estados de los drones armados, de las medidas de lucha contra la financiación del terrorismo para atacar a la sociedad civil y a los agentes humanitarios, o de las tecnologías de vigilancia. El Consejo de Seguridad y la Dirección

[13] Véase A/73/361.

[14] Véase Eric Rosand, Alistair Millar y Naureen Chowdhury Fink, “Counter-terrorism and the United Nations Security Council since 9/11: moving beyond the 2001 paradigm”, Securing the Future Initiative, septiembre de 2022.

[15] Véase https://www.un.org/securitycouncil/ctc/news/delhi-declaration-countering-use-new-and-emerging-technologies-terrorist-purposes-now-available.

Ejecutiva del Comité contra el Terrorismo deberían actuar con mucha cautela y evitar impulsar cualquier orientación demasiado restringida en materia de regulación, aunque fuera de carácter no vinculante. La orientación que las Naciones Unidas proporcionan sobre estas tecnologías se vería gravemente empobrecida si el diálogo sobre la regulación fuera dirigido únicamente —o principalmente— por un órgano de lucha contra el terrorismo que operara en un contexto de referencia limitado y pasara por alto el contexto multisectorial y multidimensional más amplio que es esencial para la regulación y la orientación y que se basa en el respeto del estado de derecho y el cumplimiento de la Carta. A la Relatora Especial le preocupa que dicha orientación entre en conflicto con los avances jurídicamente vinculantes sobre estas cuestiones que se realicen en foros paralelos o que surjan de otros procesos multilaterales más amplios, o que los socave.

16. A modo de ejemplo, el Consejo de Seguridad, en virtud de su amplia resolución 2396 (2017), exigió a los Estados (en virtud del Capítulo VII) que elaboraran sistemas de recogida de datos biométricos en contextos de lucha contra el terrorismo y creó un mandato mundial sobre la recogida, el almacenamiento, el uso y la transferencia de datos biométricos de alto riesgo sin apenas realizar consultas externas con expertos técnicos y otras partes interesadas (incluidos los Estados afectados)[16]. El fenómeno de los combatientes (terroristas) extranjeros provenientes específicamente del Iraq y de la República Árabe Siria ha sido la razón por la que se ha creado este mandato. No debe minimizarse la magnitud de las preocupaciones políticas y de seguridad en aquel momento (2014), cuando los servicios de inteligencia informaron del movimiento de (potencialmente) cientos de combatientes afiliados a grupos designados como terroristas. Sin embargo, la creación de un mandato mundial sobredimensionado para recoger los datos biométricos de cada persona que cruce una frontera en todo el planeta, basado en una amenaza regional tan específica, plantea cuestiones fundamentales sobre la proporcionalidad de la respuesta. Actualmente no se dispone de datos globales precisos sobre el número real de combatientes (terroristas) extranjeros que cruzan fronteras, y ello a pesar de que este fenómeno se invoca para justificar el establecimiento de un mandato global de recogida de datos biométricos y la adopción de otras medidas de seguridad intrusivas[17]. Así pues, la recogida de datos biométricos en las fronteras, que en un principio encontró justificación en la amenaza terrorista, se ha convertido hoy día en un medio para controlar a los migrantes[18] y proporcionar datos de vigilancia a los Estados, funcionando como mecanismo de control social. Las disposiciones relativas a la recogida de datos biométricos contenidas en la resolución 2396 (2017) se distinguen por su falta de especificidad en materia de derechos humanos y estado de derecho, además de ser gravemente perjudiciales para los derechos humanos. La aplicación de esta recogida de datos biométricos bajo una supervisión apenas superficial de los derechos humanos contribuye a agravar la lacra mundial que supone el uso indebido sistémico de las medidas antiterroristas[19]. La incapacidad de armonizar el mandato mundial de lucha contra el terrorismo con las prácticas de seguridad nacionales es una de las principales lagunas que presenta la concepción de la seguridad centrada en las Naciones Unidas, que socava la labor más amplia que realizan las Naciones Unidas en materia de desarrollo, gobernanza y estado de derecho. Resulta preocupante que los organismos regionales no hayan intervenido en medida suficiente para colmar las lagunas existentes en materia de derechos humanos y estado de derecho.

17. La Relatora Especial señala que muchas de las nuevas tecnologías implican sistemas complejos que entrañan riesgos inherentes para la protección de los derechos, en particular los de los grupos vulnerables. El hecho de que no se tengan en cuenta las características específicas de los sistemas de alto riesgo, la desvalorización sistémica de los riesgos de

[16] Véase A/73/361.

[17] Véase la resolución 2482 (2019) del Consejo de Seguridad.

[18] La Relatora Especial reconoce la labor realizada para que la recogida de los datos biométricos de los migrantes en las fronteras se lleve a cabo de forma responsable. Véase Organización Internacional para las Migraciones, “IOM and biometrics: supporting the responsible use of biometrics”, noviembre de 2018; y Katia Lindskov Jacobsen, “Biometric data flows and unintended consequences of counterterrorism”, *Revista Internacional de la Cruz Roja*, núm. 916-917 (febrero de 2022).

[19] Véase A/HRC/40/52; véanse también las comunicaciones OTH 229/2021, ISR 11/2021, IRL 3/2022 y CHN 12/2022. Todas las comunicaciones y las correspondientes respuestas que se mencionan en el presente informe pueden consultarse en https://spcommreports.ohchr.org/Tmsearch/TMDocuments.

discriminación y desigualdad y la falta de estrategias de gestión de riesgos basadas en los derechos humanos representan los principales retos en materia de derechos humanos en este ámbito. Además, se observa una escasa voluntad política de reducir los riesgos que entrañan ciertas tecnologías profundamente peligrosas, así como una escasa disposición a establecer moratorias sobre su uso. En su lugar, prevalece una actitud permisiva ante el desarrollo y el uso por parte del sector privado de nuevas tecnologías en contextos de seguridad. En definitiva, ante la falta de una definición de terrorismo acordada internacionalmente[20] y el abuso arraigado y sistémico en los distintos países de leyes y prácticas de seguridad y lucha contra el terrorismo, el uso de las nuevas tecnologías en este problemático ámbito plantea múltiples desafíos interseccionales en materia de derechos humanos.

A. Biometría

18. La biometría es la disciplina científica que se ocupa de las mediciones y los parámetros relacionados con características biológicas o de comportamiento que son comunes a todos los seres humanos y, al mismo tiempo, son claramente distintivas de una persona, lo cual permite su identificación. Estos marcadores pueden estar relacionados con las características fisiológicas de una persona, como las huellas dactilares o palmares, el ADN y el rostro, el iris o la retina (lo que se conoce como biometría biológica). Otros están vinculados a patrones de comportamiento, como el reconocimiento basado en la forma de andar de una persona (biometría del comportamiento o conductual). Dado que los atributos biométricos de la identidad son propios de la persona y, a la vez, se mantienen estables con el paso del tiempo, ofrecen una herramienta de especial utilidad para que los sistemas de identificación y autenticación de personas sean precisos y eficaces. Sin embargo, son también esas características las que hacen que los datos en cuestión sean particularmente delicados[21], por lo que, a fin de mitigar el riesgo de que se pueda acceder a ellos sin autorización, se necesitan sistemas seguros de almacenamiento y tratamiento de datos[22].

19. Las herramientas biométricas se han convertido en un instrumento habitual de las fuerzas del orden público y los organismos administrativos en varias esferas, como por ejemplo la identificación civil, la justicia penal y la gestión de fronteras. La Relatora Especial recuerda que, si bien las herramientas biométricas se han utilizado provechosamente con fines legítimos de interés público, también se han empleado en relación con graves violaciones de los derechos humanos, crímenes atroces y regímenes opresivos y autoritarios[23].

20. La Relatora Especial, entre otros, ha manifestado su inquietud por la recogida de datos biométricos de poblaciones y personas vulnerables en entornos diversos. La recogida de datos biométricos de poblaciones que se encuentran en zonas de conflicto, como por ejemplo el Iraq y el Afganistán, ha suscitado graves preocupaciones[24], en particular con respecto al hecho de que los datos biométricos que se han obtenido en el contexto de la lucha contra el terrorismo pasen directamente a manos de grupos o personas considerados terroristas por las Naciones Unidas[25]. Titulares de mandatos de los procedimientos especiales y el Comité para

[20] E/CN.4/2006/98 (párrs. 26 a 50 y 72).

[21] Según la Organización Internacional de Normalización, una característica biométrica se define como toda característica biológica o de comportamiento de una persona de la que pueden extraerse rasgos biométricos distintivos y repetibles con fines de reconocimiento biométrico (ISO/IEC 2382-37:2017(en)).

[22] Krisztina Huszti-Orbán y Fionnuala Ní Aoláin, “Use of biometric data to identify terrorists: best practice or risky business?”, University of Minnesota, 2020.

[23] United States Holocaust Memorial Museum, “Tattoos and numbers: the system of identifying prisoners at Auschwitz”, Holocaust Encyclopedia.

[24] Véase Oficina de Rendición de Cuentas del Gobierno de los Estados Unidos, “DOD biometrics and forensics: progress made in establishing long-term deployable capabilities, but further actions are needed”, informe a las comisiones del Congreso GAO-17-580 (agosto de 2017); y Electronic Privacy Information Center, “Iraqi biometric identification system” (puede consultarse en https://epic.org/privacy/biometrics/iraq.html).

[25] Después de que las Fuerzas de la Coalición se retiraran del Afganistán en agosto de 2021, los talibanes pudieron acceder a los dispositivos biométricos que habían dejado las fuerzas estadounidenses, con lo que lograron disponer de gran cantidad de datos biométricos personales.

la Eliminación de la Discriminación Racial han planteado su preocupación por el uso de estas tecnologías en la Región Autónoma de Xinjiang Uigur, en el ámbito de la Ley de Lucha contra el Terrorismo y las medidas adoptadas por China para aplicarla en la región[26]. Entre las diversas medidas que generan gran preocupación con respecto a los derechos humanos, hay informaciones que señalan que las autoridades han llevado a cabo una recogida en masa de datos biométricos (como muestras de ADN, huellas dactilares, imágenes del iris y grupos sanguíneos) de residentes de la región. El uso de datos biométricos en Somalia y por Israel en el Territorio Palestino Ocupado ha despertado inquietudes similares[27].

21. La Relatora Especial destaca que la pandemia de enfermedad por coronavirus (COVID-19) ha acelerado la recogida de datos biométricos y ha acentuado tanto la excepcionalidad como la normalidad de su uso, ya que se han utilizado las capacidades biométricas concebidas con fines antiterroristas y de seguridad para la gestión de una pandemia sanitaria mundial que ha afectado de manera desproporcionada a las minorías religiosas, étnicas y raciales, a otros grupos vulnerables y a las personas marginadas económica y socialmente[28]. El hecho de que las capacidades biométricas desarrolladas para luchar contra el terrorismo se destinen a gestionar a las comunidades más marginadas durante una pandemia debería preocupar a todas las partes interesadas.

22. El uso creciente (y el uso indebido) de la tecnología biométrica en el contexto de la lucha contra el terrorismo es una cuestión que se trata en varias resoluciones del Consejo de Seguridad. En su resolución 2396 (2017), el Consejo pidió a los Estados que “elaboren y apliquen sistemas de recogida de datos biométricos” a fin de “verificar debidamente y de forma responsable la identidad de los terroristas, incluidos los combatientes terroristas extranjeros”. En esa resolución, el Consejo pidió explícitamente a los Estados que elaboraran y aplicaran sistemas de recogida de datos que podrían incluir la toma de huellas dactilares, la fotografía, el reconocimiento facial y otras formas de recogida de datos biométricos pertinentes[29].

23. Este esfuerzo normativo concertado a favor de una recogida sistemática de datos biométricos no se ha visto acompañado de la labor necesaria para establecer un régimen jurídico y reglamentario adecuado a escala mundial. De hecho, en lugar de encabezar una iniciativa global para acordar un conjunto de reglas y normas internacionales sólidas en materia de recogida de datos biométricos y de identificación, el principal empeño del sistema de las Naciones Unidas se ha limitado a la creación de un programa de fomento de la capacidad para facilitar esa recogida: el Programa de las Naciones Unidas de Lucha contra los Viajes de Terroristas. Este programa comprende, entre otras cosas, la prestación de asistencia técnica y apoyo a los Estados miembros en su labor de recogida de conjuntos de datos relativos a la información anticipada sobre los pasajeros y el registro de nombres de los pasajeros de todas las personas que viajan por vía aérea a escala internacional, con el respaldo del programa informático goTravel de las Naciones Unidas, que la Organización proporciona a los Estados como herramienta normalizada para la recogida, el intercambio y el análisis de datos[30].

24. Entre las inquietudes concretas que plantea la Relatora Especial con respecto al Programa y el sistema de recogida de datos personales al que presta apoyo figuran las siguientes: a) la recogida de datos en principio, habida cuenta del grado de detalle que ofrecen los datos, en particular los datos del registro de nombres de los pasajeros, sobre la vida de los

[26] Véanse las comunicaciones CHN 18/2019 y CHN 14/2020; y CERD/C/CHN/CO/14-17, párr. 40 b).

[27] Véase Keren Weitzberg, “Biometrics and counter-terrorism: case study of Somalia”, Privacy International, mayo de 2021; y la comunicación ISR 11/2021.

[28] Fionnuala Ní Aoláin, “Exceptionality: a typology of COVID-19 emergency powers”, *UCLA Journal of International Law and Foreign Affairs*, vol. 26, núm. 2 (2022).

[29] Se han publicado algunas orientaciones de las Naciones Unidas sobre el uso de datos biométricos en la lucha contra el terrorismo, pero la Relatora Especial considera que se deben revisar a fondo para que tengan en cuenta los aspectos relacionados con los derechos humanos y los riesgos que entraña el uso generalizado de datos biométricos por los Estados. Véase https://www.unodc.org/pdf/terrorism/Compendium-Biometrics/Compendium-biometrics-final-version-LATEST_18_JUNE_2018_optimized.pdf.

[30] Véanse https://learn.unoct-connectandlearn.org/course/index.php?categoryid=35 y https://www.un.org/cttravel/goTravel.

interesados; b) el hecho de que la recogida de datos, por definición y de forma inevitable, se realice con respecto a todos los pasajeros sin discriminación, lo cual supone un evidente problema en lo que respecta a la necesidad y la proporcionalidad; c) la duración del período de conservación, que da lugar a que el uso de esos datos no se limite a una mera comprobación de las listas de vigilancia para determinados vuelos, sino que pueda convertirse en un registro a largo plazo de comportamientos personales del que pueden extraerse informaciones detalladas; y d) el intercambio transfronterizo de datos entre organismos de distintas naciones entraña riesgos específicos con respecto a los distintos grados de cumplimiento de los derechos humanos a escala internacional. La Relatora Especial está profundamente preocupada por el carácter inexacto y discriminatorio de las decisiones basadas en algoritmos en los mecanismos de información anticipada sobre los pasajeros y los registros de nombres de los pasajeros. A ese respecto, hace hincapié en que el uso o la transferencia de estas tecnologías puede tener repercusiones en la libertad de circulación, el derecho a salir de cualquier país y el derecho a solicitar asilo, y destaca que los Estados a los que se transfieren los datos los utilizan de forma ilegítima para dirigirse contra determinados objetivos y que los recursos que existen contra las violaciones de los derechos humanos que se producen en el contexto del uso de esos datos son totalmente inadecuados[31]. La Relatora Especial observa asimismo que el Programa colabora de forma limitada con las entidades de derechos humanos de las Naciones Unidas y pide que se someta a una auditoría independiente para garantizar la integridad de sus prácticas y la transferencia de tecnología en lo relativo a los derechos humanos, la protección de datos y el estado de derecho.

25. En ese mismo sentido, la Relatora Especial manifiesta su gran preocupación por el papel que desempeña y la influencia que ejerce el Biometrics Institute, una organización con sede en el Reino Unido dedicada a la promoción de normas y prácticas, y que se muestra cercana a la industria y a los Gobiernos, pero sumamente cerrada e inaccesible a los agentes de la sociedad civil y a las partes interesadas en los derechos humanos[32].

26. La Relatora Especial también subraya su honda inquietud por el intercambio de datos biométricos, una práctica que la comunidad internacional alienta enérgicamente. Un aspecto llamativo de la reglamentación normativa de la lucha contra el terrorismo ha sido la creciente importancia que se concede a la cooperación entre los Estados a fin de promover los supuestos intereses comunes en la materia[33]. El intercambio de datos es un ámbito opaco de la práctica del derecho internacional, ya que no se dispone de mucha información sobre si se intercambian datos biométricos y de qué tipo y, más concretamente, sobre el contenido de los acuerdos de intercambio de datos. Se desconoce en gran medida si en esos acuerdos figuran consideraciones relativas a los derechos humanos. La Relatora Especial resalta la tensión que existe actualmente entre, por un lado, los reiterados llamamientos de la Asamblea General y el Consejo de Derechos Humanos a la cooperación antiterrorista entre los Estados, en instrumentos que van desde la Estrategia Global de las Naciones Unidas contra el Terrorismo hasta algunas resoluciones[34], y, por el otro, el hecho de que se omita por completo especificar que esa cooperación debe llevarse a cabo respetando las obligaciones de los Estados en materia de derechos humanos, en particular con respecto al derecho a la privacidad.

B. Drones

27. Otro campo en el que se aprecia claramente la tendencia a normalizar e incorporar el uso habitual de tácticas y tecnologías que son problemáticas y, en ocasiones, ilegales, concebidas originalmente con fines excepcionales y específicos de lucha contra el terrorismo y protección de la seguridad nacional, es el de los drones. La tecnología de los drones está creciendo a un ritmo notable. El uso de drones armados en todo el mundo, tanto en el marco

[31] ACNUDH, “Principios y Directrices recomendados sobre los derechos humanos en las fronteras internacionales” (octubre de 2014), p. 14.

[32] Véase https://www.biometricsinstitute.org/.

[33] Resolución 2482 (2019) del Consejo de Seguridad, párr. 15 c), y resoluciones de la Asamblea General 75/291, párr. 30, y 60/288, anexo, secc. II, párrs. 3 a 5.

[34] Véase la resolución 76/169 de la Asamblea General y la resolución 51/24 del Consejo de Derechos Humanos.

de conflictos armados formales en determinadas ubicaciones geográficas como en el marco de una supuesta respuesta antiterrorista, sigue siendo objeto de gran controversia y representa un riesgo constante para la población civil, además de un obstáculo para la protección de los derechos humanos. Los ataques con drones se han utilizado tanto contra objetivos situados en zonas de guerra durante el conflicto como contra determinadas personas, mediante los denominados "asesinatos selectivos" cometidos fuera del entorno geográfico del conflicto. Muchos de esos conflictos son singulares, ya que no se definen como conflictos armados internacionales clásicos, sino como escenarios de operaciones y prácticas de lucha contra el terrorismo. El desarrollo de la tecnología de los drones está indisolublemente ligado a la capacidad y la letalidad de las fuerzas militares[35], y los ataques con drones se han justificado de forma sistemática desde el punto de vista de la lucha contra el terrorismo. El uso de las operaciones con drones ha sido objeto de duras críticas, en particular por la Relatora Especial sobre las ejecuciones extrajudiciales, sumarias o arbitrarias y el ex Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo[36]. La Relatora Especial se suma a esas condenas y cuestiona la legalidad del uso extraterritorial de drones letales y las numerosas violaciones de los derechos humanos que conllevan esas operaciones. Manifiesta asimismo su profundo malestar ante la creciente utilización de los drones que pueden volar más lejos de lo que el operador puede ver a simple vista (llamados en ocasiones drones "más allá del horizonte"), con el supuesto fin de prevenir el terrorismo. La Relatora Especial advierte del riesgo de que se perpetúen las condiciones que propician el terrorismo, en las que el uso de la fuerza es pernicioso, no rinde cuentas, es indiscriminado en la práctica y está motivado por una arrogancia que desvaloriza la vida de quienes se encuentran sobre el terreno[37].

28. A pesar de los intentos que se han hecho en la última década para instar a los Estados a que acuerden, adopten y cumplan normas coherentes sobre el uso lícito de los drones armados, se han logrado pocos avances tangibles al respecto. Los Estados han seguido utilizando esta tecnología como medio para el asesinato selectivo de presuntos terroristas en el exterior, tanto dentro como fuera del marco formal del conflicto armado. Además, muchos Estados han empezado a ampliar el uso de los drones armados dentro de sus propias fronteras, y se han desarrollado nuevas tecnologías, como los nanodrones, los drones armados con armas no letales y los drones letales no incendiarios, que plantean nuevas inquietudes en materia de derechos humanos. La Relatora Especial destaca la ausencia de una reglamentación completa en este ámbito impulsado por la innovación, en particular la falta absoluta de protección y aplicación de los derechos humanos.

29. La Relatora Especial recuerda la labor realizada en relación con el uso de drones armados por anteriores titulares de mandatos. En el informe que presentó en 2013 a la Asamblea General[38], Ben Emmerson examinó decenas de ataques, perpetrados desde el Afganistán hasta el Territorio Palestino Ocupado entre 2001 y 2013, y destacó la preocupante falta de transparencia en el uso de drones armados, lo cual, en palabras de la Alta Comisionada de las Naciones Unidas para los Derechos Humanos "crea un vacío de responsabilidad y afecta a la capacidad de resarcimiento de las víctimas"[39]. En el informe que presentó en 2014 al Consejo de Derechos Humanos, el Sr. Emmerson subrayó que existía una necesidad urgente e imperiosa de que los Estados alcanzaran un consenso sobre una serie de cuestiones a fin de promover la protección de los derechos humanos y el derecho humanitario[40]. La Relatora Especial reitera el llamamiento que hizo el Secretario General en favor de una prohibición mundial de los sistemas de armas autónomos letales[41].

30. La Relatora Especial hace hincapié en que la aplicabilidad de las normas jurídicas internacionales relativas al uso legítimo de la fuerza no es una cuestión abstracta ni una

[35] Imperial War Museum, "A brief history of drones". Puede consultarse en https://www.iwm.org.uk/history/a-brief-history-of-drones.

[36] Véanse A/HRC/44/38, A/HRC/25/59, A/HRC/14/24/Add.6 y A/68/389.

[37] Véase Atef Abu Saif, *The Drone Eats With Me: A Gaza Diary* (Boston, Beacon Press, 2016).

[38] A/68/389.

[39] *Ibid.*, párr. 41.

[40] A/HRC/25/59, párr. 71.

[41] Véase https://www.un.org/sg/en/content/sg/statement/2018-11-11/allocution-du-secrétaire-général-au-forum-de-paris-sur-la-paix.

cuestión ajena a la evaluación que debe hacerse, desde el punto de vista de los derechos humanos, de los ataques letales con drones. Como principio básico del derecho internacional de los derechos humanos, el uso de la fuerza letal para privar a una persona del derecho a la vida debe ejercerse en todos los casos de forma no arbitraria. Como señaló el Comité de Derechos Humanos en su observación general núm. 36 (2019), el derecho a la vida es "el derecho supremo respecto del cual no se permite suspensión alguna, ni siquiera en situaciones de conflicto armado u otras situaciones de emergencia pública que amenacen la vida de la nación" y la privación de la vida es arbitraria "si es incompatible con el derecho internacional o la legislación interna". El Comité observó además que "el uso de la fuerza letal de manera compatible con el derecho internacional humanitario y otras normas del derecho internacional vigentes no es, en general, arbitrario" y, por lo tanto, "los Estados partes deberían, en general, revelar los criterios que justifiquen el uso de la fuerza letal contra personas o bienes cuyo resultado pueda ser la privación de la vida, por ejemplo los fundamentos jurídicos de ataques específicos, (...) las circunstancias en que se hayan utilizado los medios y métodos de guerra pertinentes y si se consideraron alternativas menos lesivas"[42]. Cuando los Estados se basan en supuestas justificaciones que no pueden ampararse de forma adecuada en el derecho internacional, sus acciones violan, por definición, el principio fundamental de los derechos humanos de la no arbitrariedad. La Relatora Especial está profundamente preocupada por que el uso extraterritorial que se está haciendo actualmente de los drones armados implique un uso arbitrario de la fuerza en virtud de las normas del derecho internacional de los derechos humanos.

31. En los últimos cinco años, la tecnología de los drones ha seguido la misma trayectoria que se ha observado en las tácticas policiales y el armamento en general, pasando del campo de batalla al frente interno. Este paso, que entraña dejar de justificar su uso en el contexto del conflicto y la lucha contra el terrorismo para integrarlo en la aplicación "ordinaria" de la ley, sigue el modelo sistemático que se señala en el presente informe, por el que los métodos que en un principio se justificaban por objetivos excepcionales de lucha contra el terrorismo se incorporan gradualmente al ordenamiento jurídico local, nacional y "ordinario". Más en concreto, después de que la Autoridad Federal de Aviación de los Estados Unidos adoptara en 2016 una norma que permite el uso de drones en el espacio aéreo civil del país[43], su utilización por los organismos nacionales encargados de hacer cumplir la ley, primero en los Estados Unidos y después en todo el mundo, se ha extendido rápidamente. Hay estudios que indican que, en los Estados Unidos, más de 1.000 departamentos de policía utilizan actualmente la tecnología de los drones[44]. En el Reino Unido, utilizan drones al menos 40 fuerzas policiales[45]. Las fuerzas policiales en China utilizan drones, y la Oficina de Seguridad Pública de Xinjiang se ha asociado con la empresa DJI, el principal fabricante de drones del mundo, que controla más del 75 % del mercado de drones[46]. También los están utilizando fuerzas policiales en Australia e Israel, y en África, Europa, el golfo Pérsico y las Américas[47].

32. Cabe resaltar que, en varios contextos nacionales, el uso de los drones se justifica por razones de seguridad nacional y de lucha contra el terrorismo, con el argumento de que son necesarios para combatir el terrorismo en el país o para proteger de atentados terroristas infraestructuras de importancia crítica. La primera generación de drones que utilizaron en el plano nacional las fuerzas del orden solo desempeñaba funciones de vigilancia. Se trataba, en la práctica, de cámaras de circuito cerrado de televisión que navegaban por el cielo. Sin

[42] Comité de Derechos Humanos, observación general núm. 36 (2019), párrs. 2, 12 y 64.

[43] Véase https://www.faa.gov/newsroom/faa-doubles-blanket-altitude-many-uas-flights?newsId=852644.

[44] Véase https://atlasofsurveillance.org/atlas.

[45] Véase Chris Cole y Jonathan Cole, "Benchmarking police use of drones in the UK", UK Drone Watch, 2 de noviembre de 2020.

[46] Véase Departamento del Tesoro de los Estados Unidos, "Treasury identifies eight Chinese tech firms as part of the Chinese military-industrial complex", 16 de diciembre de 2021; y Blake Schmidt y Ashlee Vance, "DJI won the drone wars, and now it's paying the price", *Businessweek*, 26 de marzo de 2020.

[47] Véase Christof Heyns, "Human rights and the use of autonomous weapons systems (AWS) during domestic law enforcement", *Human Rights Quarterly*, vol. 38, núm. 2, págs. 350–378; y Policía Federal Australiana, "Australia and Sri Lanka strengthen ties over aerial drone surveillance", 9 de abril de 2021.

embargo, la generación actual suele estar equipada con prestaciones más avanzadas, como visión termográfica y nocturna, seguimiento automático de objetivos, altavoces y focos. Los fabricantes de drones han desarrollado modelos destinados al mercado policial equipados con armas no letales. Algunos fabricantes franceses de drones comercializan modelos para las fuerzas del orden que pueden transportar hasta 18 granadas de gas lacrimógeno[48]. Un fabricante sudafricano de drones, Desert Wolf, ha creado un dron con cañones de bolas de pintura de gran capacidad que pueden disparar proyectiles sólidos, bolas de pintura o gas pimienta[49]. El argumento de venta de este tipo de armas está directamente relacionado con la articulación de riesgos y amenazas para la seguridad nacional, tanto desde dentro como desde fuera del país. La Relatora Especial recuerda a las empresas que tienen la responsabilidad de respetar todos los derechos humanos internacionalmente reconocidos. Las empresas deben abstenerse de infringir los derechos humanos de terceros y hacer frente a las consecuencias negativas que generan sobre los derechos humanos. Básicamente, los Estados deben exigir responsabilidades a las empresas por las violaciones de los derechos humanos. El segundo pilar de los Principios Rectores sobre las Empresas y los Derechos Humanos proporciona un plan oficial aplicable a todas las empresas para dar cumplimiento a esa responsabilidad[50].

33. A medida que la tecnología de los drones se vuelva más sofisticada, es probable que los operadores pasen a utilizar micro o nanodrones, lo cual tendrá consecuencias de gran alcance para los derechos humanos, ya que su despliegue será más fácil y su capacidad de intrusión será mayor. El dron Black Hornet, desarrollado por la empresa noruega Prox Dynamics, ya es utilizado oficialmente por unas 20 fuerzas militares, entre ellas la Infantería de Marina de los Estados Unidos, el Ejército británico y las fuerzas armadas de Alemania, Australia, Francia, Sudáfrica y Türkiye . El dron Black Hornet pesa menos de 20 gramos, cabe en una mano y vuela prácticamente en silencio. Los modelos actuales pueden ir equipados con cámaras para capturar imágenes fijas y en movimiento, con un alcance de1,6 km. Las fuerzas militares han utilizado miles de microdrones de este tipo en los últimos cinco años[51].

34. Además, la Relatora Especial está profundamente preocupada por el uso de drones para vigilar las protestas. A ese respecto, subraya una vez más que esta práctica se inscribe dentro de la tendencia más general que ha constatado en lo que se refiere al uso excepcional de determinadas tecnologías, que ha sido efímero, y que ahora se ha reorientado hacia un uso ordinario por el Estado. Además de sus evidentes implicaciones para la privacidad, la libertad de reunión, la libertad de expresión y el derecho a participar en los asuntos políticos, el uso de drones, combinado con el poder coercitivo de la policía, pone sobre la mesa cuestiones relacionadas con la detención arbitraria, la libertad y la seguridad de la persona y el derecho a la vida.

35. Teniendo en cuenta que la tecnología de los drones en el plano nacional avanza en la dirección de las capacidades armadas, es necesario garantizar que el marco de derechos humanos que acompaña a las operaciones que ponen en peligro los derechos del objetivo a la seguridad y a la vida se convierta en parte de los procedimientos operativos estándar de las fuerzas del orden en todo el mundo. Es necesario extraer enseñanzas de las consecuencias negativas que se han derivado del uso de los drones en contextos de lucha contra el terrorismo y aplicarlas a su posible uso en entornos de mantenimiento del orden público a escala nacional. La primera parte de ese marco consiste en que las fuerzas del orden tienen la

[48] Véase Christian Enemark, “Armed drones and ethical policing: risk, perception, and the tele-present officer”, *Criminal Justice Ethics*, vol. 40, núm. 2, págs. 124–144. Véase, por ejemplo, Drone Volt’s Hercules 10 tear gas model (puede consultarse en https://www.aeroexpo.online/prod/drone-volt/product-180237-28892.html).

[49] Véase Leo Kelion, “African firm is selling pepper-spray bullet firing drones’, *BBC News*, 18 de junio de 2014.

[50] A/HRC/48/31, párr. 11.

[51] Véanse https://www.flir.co.uk/news-center/military/flir-wins-additional-$15.4m-contract-for-black-hornet-nano-uav-systems-for-u.s.-army-soldier-borne-sensor-program/; https://www.flir.fr/news/press-releases/flir-systems-awarded-$89-million-contract-from-french-armed-forces-to-deliver-black-hornet-personal-reconnaissance-system/; y https://www.regjeringen.no/en/aktuelt/droner/id2924942/?fbclid=IwAR0-lEUzOY5c5gorr6nY0-xBcqyGfgpCzzWQxb55Xgg9OniVOkKThv1Fumw.

obligación de llevar a cabo una planificación previa, y no limitarse a utilizar drones como práctica habitual o cuando los agentes lo prefieren. Las obligaciones relativas a la planificación de operaciones que podrían resultar nocivas se han recogido en la jurisprudencia, como en el asunto *McCann y otros c. el Reino Unido*, del Tribunal Europeo de Derechos Humanos. El Tribunal sostuvo en ese asunto que los riesgos a la vida se deben someter "al examen más minucioso, en particular cuando se utiliza deliberadamente la fuerza letal, tomando en consideración no solo las acciones de los agentes del Estado que administran efectivamente la fuerza, sino también todas las circunstancias concurrentes, como la planificación y el control de las acciones en cuestión"[52]. Los factores que deben tenerse en cuenta en la planificación son señalados por el Comité de Derechos Humanos en el párrafo 12 de su observación general núm. 36, en el que se dispone que toda acción que entrañe un riesgo de muerte o de lesiones graves "debe resultar estrictamente necesaria habida cuenta de la amenaza".

36. Si los drones van a utilizarse de manera que entrañen un riesgo de muerte o lesiones graves, los organismos estatales encargados de hacer cumplir la ley deben estar en condiciones de cumplir con la obligación que les incumbe con arreglo a las normas de derechos humanos de llevar a cabo la debida investigación (ampliamente reconocida a escala internacional por el Comité de Derechos Humanos[53], la Corte Interamericana de Derechos Humanos[54] y la Comisión Africana de Derechos Humanos y de los Pueblos[55]). Las características fundamentales de la obligación de investigación se han establecido con rigor en la versión revisada del Protocolo de Minnesota sobre la Investigación de Muertes Potencialmente Ilícitas. Entre ellas, se pueden destacar las siguientes:

a) La investigación debe ser pronta;

b) La investigación debe ser efectiva y exhaustiva;

c) Las investigaciones y las personas que las llevan a cabo también deben ser independientes de influencias indebidas, además de ser percibidas como tales, y los investigadores deben ser imparciales y actuar en todo momento de manera desinteresada;

d) Las investigaciones de violaciones de los derechos humanos deben ser transparentes, lo que supone estar abiertos al escrutinio del público en general y de las familias de las víctimas.

37. Es evidente que existe el riesgo de que la tecnología de los drones utilizada en el ámbito de las fuerzas del orden rebase los límites y sea adoptada en otros ámbitos y por otros actores. Se trata de algo que ya hemos visto en el contexto de la lucha contra el terrorismo. La proliferación de la tecnología de los drones está impulsada por un grupo restringido de Estados, pero estos no pueden tener la certeza de que serán capaces de controlar la futura difusión de dicha tecnología. Una preocupación importante de la Relatora Especial es el proceso por el cual las Naciones Unidas y los Estados colaboran y proporcionan asesoramiento técnico y creación de capacidades en todo el mundo, también mediante la transferencia de tecnología, como los drones[56]. Los Estados pueden realizar transferencias de tecnología de forma intencionada y consciente, pero también pueden hacerlo por fallos en la diligencia debida que propicien transferencias accidentales, oportunistas o encubiertas de tecnología y capacidades. Los Estados que disponen de herramientas potentes tienen la importante obligación de salvaguardarlas y evitar que caigan en manos ajenas. Al promover el uso de esas tecnologías en los Estados, las Naciones Unidas también están sujetas a responsabilidades como la política de diligencia debida en materia de derechos humanos. La trayectoria de los Estados en lo que respecta a mantener bajo control la tecnología de los drones deja mucho que desear. Como señaló la Relatora Especial sobre las ejecuciones extrajudiciales, sumarias o arbitrarias, al menos 20 agentes no estatales han conseguido

[52] Tribunal Europeo de Derechos Humanos, *McCann and others v. the United Kingdom*, demanda núm. 18984/91, sentencia de 27 de septiembre de 1995, párr. 150.

[53] Observación general núm. 31, párrs. 15 y 18.

[54] *Caso Montero Aranguren y otros (Retén de Catia) Vs. Venezuela*, Serie C No. 150, sentencia de 5 de julio de 2006, párr. 66.

[55] Observación general núm. 3, párrs. 2 y 15.

[56] Véase A/76/261.

sistemas de drones armados y no armados, entre ellos el Ejército Nacional Libio, Harakat Tahrir al-Sham, la Yihad Islámica Palestina, desertores militares venezolanos, el Partido de los Trabajadores del Kurdistán (PKK), el Grupo Maute, el Cártel de Jalisco Nueva Generación, el movimiento huzí y el Dáesh [57]. Los Estados están empezando a enfrentarse gradualmente a las implicaciones que tiene el uso de drones por grupos delictivos o no estatales. En abril de 2022, el Gobierno de los Estados Unidos puso en marcha su plan nacional de lucha contra los sistemas aéreos no tripulados, destinado a responder al uso malintencionado de drones por parte de agentes internos hostiles[58].

C. La inteligencia artificial en la lucha contra el terrorismo

38. La Relatora Especial reconoce que el uso de la IA aumenta rápidamente, y está cambiando múltiples esferas de la actividad social, económica, política y militar. Entiende que la IA tiene las propiedades de una tecnología de uso general, lo que significa que abrirá amplias posibilidades de aplicación. La Relatora Especial afirma que los Estados cada vez incorporan más sistemas de IA en sus sistemas de aplicación de la ley, seguridad nacional, justicia penal y gestión de fronteras[59].

39. Los algoritmos son el eje del desarrollo y el uso de la IA, que, en estos contextos, funciona como herramienta de predicción. En el ámbito de la lucha contra el terrorismo, los sistemas de IA utilizan cantidades ingentes de datos, por ejemplo de carácter histórico, de justicia penal, de viajes y comunicaciones, medios sociales y salud. Las tecnologías pueden utilizarse para crear perfiles de personas, identificar lugares susceptibles de albergar una mayor actividad delictiva o terrorista, o señalar a individuos como presuntos sospechosos y futuros reincidentes[60]. El uso de la IA tiene consecuencias directas para el individuo en lo que respecta a la relación personal con el poder del Estado, incluida su capacidad coercitiva. Las repercusiones para la privacidad y los derechos humanos de este tipo de recopilación de datos y actividad de predicción son profundas, tanto para los derechos derogables como para los inderogables. La Relatora Especial resalta su profunda inquietud por el hecho de que se estén utilizando evaluaciones de IA para desencadenar la acción del Estado en contextos de lucha antiterrorista, desde registros, interrogatorios, detenciones, enjuiciamientos y medidas administrativas hasta una vigilancia más profunda e intrusiva, pese a que las evaluaciones de IA por sí mismas no deberían ser motivo de sospecha razonable, dada su naturaleza inherentemente probabilística. La Relatora Especial coincide con el ACNUDH en que la opacidad de la toma de decisiones basada en la IA supone una carga excepcional para lograr la transparencia y la rendición de cuentas en materia de derechos humanos por su uso[61].

40. Además, la Relatora Especial está profundamente preocupada por la arraigada práctica de los Estados de adoptar leyes que eximen de los regímenes ordinarios de supervisión el uso de la IA con fines militares y de seguridad nacional. A este respecto, señala la exclusión recogida en el proyecto de ley sobre inteligencia artificial de la Unión Europea y en el "borrador cero" del Consejo de Europa, por ahora confidencial, de un convenio sobre IA, derechos humanos, democracia y estado de derecho. En el contexto europeo, la Relatora Especial advierte enérgicamente en contra de que la ley de IA contemple una exención general por motivos de seguridad nacional y alienta a la Unión Europea a velar por que las exenciones sean proporcionadas y acordes con la legislación vigente de la Unión Europea, incluida la Carta de los Derechos Fundamentales. Recomienda que la legislación obligue a organismos como la Agencia de la Unión Europea para la Cooperación Policial (Europol) y la Agencia Europea de la Guardia de Fronteras y Costas (Frontex) a cumplir las obligaciones de la Carta, ya que eximirlos crearía un reducto de excepcionalidad que sentaría un precedente terrible en el plano regional y mundial. Asimismo, la Relatora Especial subraya que los sistemas de IA desarrollados con fines militares o de doble uso deben estar regulados por la ley de IA. Sostiene que el convenio del Consejo de Europa debe incluir en su ámbito

[57] A/HRC/44/38, párr. 9.
[58] Véase https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/25/fact-sheet-the-domestic-counter-unmanned-aircraft-systems-national-action-plan/.
[59] Véase A/HRC/48/31.
[60] *Ibid.*, párr. 23.
[61] Véase A/HRC/48/31.

de aplicación el diseño, desarrollo y uso de sistemas de IA para la defensa nacional, puesto que, si se excluyeran, el proyecto de convenio sería irrelevante para las inquietudes de derechos humanos más destacadas de la región.

D. Vigilancia

41. La Relatora Especial está profundamente preocupada por la magnitud de las violaciones de los derechos humanos que se derivan de la proliferación y el uso indebido en todo el mundo de sofisticadas tecnologías intrusivas de cibervigilancia, cuya justificación o intención original era combatir el terrorismo y velar por la seguridad nacional. Ha elaborado un documento de posición sobre el tema para los Estados Miembros titulado "Global regulation of the counter-terrorism spyware technology trade: scoping proposals for a human rights-compliant approach"[62]. En el anexo del presente informe se resumen las recomendaciones del documento de posición, y se indican las características que deberá tener cualquier futuro marco regulador para actuar ante el comercio mundial de programas espía. La Relatora Especial es consciente de que estas tecnologías potentes e innovadoras pueden proporcionar a las fuerzas del orden y a los servicios militares y de seguridad unas poderosas herramientas de investigación y vigilancia para desbaratar los actos de violencia terrorista y llevar a los autores ante la justicia.

42. Las fuerzas gemelas del siglo XXI —rápido aumento de la capacidad y complejidad de los equipos y programas informáticos, combinado con la expansión sustancial de la financiación y prominencia de programas antiterroristas estatales— han conducido al desarrollo de una amplia gama de sofisticadas tecnologías de vigilancia dirigidas a la lucha antiterrorista o adecuadas para ella. La práctica habitual en materia de lucha antiterrorista e investigación criminal promovida por organizaciones multilaterales como el Consejo de Europa y la Organización Internacional de Policía Criminal (INTERPOL) pide que la vigilancia rutinaria y la recopilación de datos se realicen por medio de herramientas de *hardware* y *software* para el análisis de la investigación[63]. En los últimos años, varias tendencias convergentes han favorecido en gran medida la capacidad para efectuar este tipo de vigilancia masiva como herramienta habitual de investigación: la caída vertiginosa del costo de la tecnología y del almacenamiento de datos, la ubicuidad de los dispositivos digitales y la conectividad, y el aumento exponencial de la capacidad de procesamiento de las computadoras.

43. La proliferación de la industria de la tecnología de vigilancia en el siglo XXI se ha debido en parte a los importantes flujos de financiación destinados a combatir el terrorismo. Otro factor fueron los extraordinarios poderes que se arrogaron los organismos estatales con el pretexto de que las exigencias de la lucha antiterrorista justifican la vigilancia ubicua y la intrusión gubernamental como herramienta preventiva y de investigación[64]. En consonancia con las pautas fundamentales de uso señaladas en el presente informe, la intrusión suele presentarse como dirigida únicamente a determinados grupos de riesgo, que se suelen definir de forma difusa y problemática haciendo referencia a suposiciones (a menudo discriminatorias)[65] sobre el riesgo percibido de daños futuros. Esas evaluaciones del riesgo suelen basarse en pruebas empíricas deficientes o escasas y sus metodologías generalmente son poco rigurosas y no están concebidas para la tarea en cuestión. La falta de claridad o rigor de esas definiciones hace que las operaciones antiterroristas tiendan a rebasar los límites fijados inicialmente.

44. La sofisticada tecnología de vigilancia desarrollada con fines antiterroristas y de seguridad nacional se ha ido convirtiendo en un tema que suscita preocupación internacional a raíz de una sucesión de revelaciones que demuestran que, en realidad, tales herramientas se utilizan para espiar a políticos, periodistas, activistas de derechos humanos, abogados y

[62] Véase https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/2022-12-15/position-paper-unsrct-on-global-regulation-ct-spyware-technology-trade.pdf.

[63] Véase Oficina del Programa de Ciberdelincuencia del Consejo de Europa, Standard operating procedures for the collection, analysis and presentation of electronic evidence, septiembre de 2019.

[64] A/69/397, párr. 19.

[65] A/HRC/43/46, párrs. 28 a 34.

ciudadanos de a pie que no tienen ningún vínculo con el terrorismo ni suponen una amenaza para la seguridad nacional. La tecnología encubierta intrusiva que vigila el contenido de las comunicaciones digitales de las personas y otra información, como los metadatos (ubicación, duración, fuente y contactos), —conocida comúnmente como programas espía— ha proliferado a escala internacional ajena a todo control y plantea serios riesgos para la promoción y protección de los derechos humanos. Para ilustrar la magnitud del problema cabe citar el escándalo relativo al uso por parte de regímenes represivos de Pegasus, un programa informático de vigilancia fabricado por la empresa de ciberinteligencia NSO Group, que dio lugar a investigaciones a cargo del Parlamento Europeo y a litigios[66].

45. La vigilancia tiene repercusiones considerables sobre múltiples derechos humanos. La Relatora Especial subraya que el derecho a la privacidad funciona como un derecho de entrada, ya que protege y habilita otros muchos derechos y libertades. La protección de este derecho está íntimamente relacionada con la existencia y el avance de la sociedad democrática. Por ello, la Relatora Especial considera que la escalada en el uso de la vigilancia secreta y la recopilación de información sobre contenidos y metadatos con fines de lucha antiterrorista, junto con el desarrollo desbocado de nuevas tecnologías insuficientemente reguladas, constituye una amenaza seria para las sociedades democráticas.

46. La responsabilidad de estos graves problemas recae no solo en las entidades privadas que desarrollan y, o bien proporcionan a sabiendas esas tecnologías directamente a regímenes que violan los derechos o bien no ejercen la diligencia debida sobre el uso final de su producto, sino también en los organismos estatales que hacen un uso indebido de esas tecnologías vulnerando el derecho internacional y nacional, y en los Estados y las organizaciones internacionales que, o bien facilitan activamente o bien, por falta de una regulación sólida, no han impedido que, al comercializarse, esas tecnologías caigan en manos equivocadas.

47. Si bien en épocas anteriores la tecnología de espionaje y vigilancia solía ser patrimonio exclusivo de agencias estatales y de expertos técnicos internos, en la era moderna la gran mayoría de las herramientas de vigilancia que utilizan las agencias estatales se obtienen del sector privado. Algunas de las empresas privadas de ciberseguridad responsables de herramientas dotadas de esas capacidades son NSO, Quadream y Candiru/Saito Tech, las tres con sede en Israel; Gamma International, con sede en el Reino Unido; Vilicius Holding y Trovicor, con sede en Alemania; Qosmos y Amesys, con sede en Francia; Area SpA y Hacking Team/Memento Labs, con sede en Italia; la empresa Cytrox, que tiene divisiones en Hungría, Israel y Macedonia del Norte; las empresas estadounidenses CyberPoint, Narus (filial de Boeing), Blue Coat Systems y Cisco Systems; y la empresa DarkMatter, de los Emiratos Árabes Unidos. Es urgente que se regulen las actividades de estas empresas y multinacionales, con arreglo a las obligaciones de los Estados relativas a la regulación del sector empresarial, para evitar violaciones de los derechos humanos.

48. A la luz de las recientes revelaciones, cada vez son más las voces de la comunidad internacional de derechos humanos que apoyan la petición de un marco regulador más sólido y respetuoso con los derechos humanos para el uso, la venta y la transferencia de tecnología de vigilancia y, mientras tanto, una moratoria sobre el comercio y la transferencia de dicha tecnología. La Alta Comisionada de las Naciones Unidas para los Derechos Humanos ha pedido un sistema mejor, basado en los derechos humanos, para regular el comercio de programas espía, que incluya mecanismos para responsabilizar de las violaciones de los derechos humanos a los productores privados de programas espía “exigiendo por ley que las empresas implicadas cumplan con sus responsabilidades en materia de derechos humanos, sean mucho más transparentes con respecto al diseño y el uso de sus productos y pongan en marcha medidas más eficaces de rendición de cuentas[67]”. Asimismo, la Alta Comisionada ha

[66] En marzo de 2022, el Parlamento Europeo creó una comisión de investigación encargada de examinar el uso de Pegasus y otros programas espía de vigilancia equivalentes (véase https://www.europarl.europa.eu/committees/es/pega/home/highlights). Con respecto a los litigios, véase United States Federal Case No. 19-cv-07123-PJH *WhatsApp Inc. et al v. NSO Group Technologies Ltd et al.*

[67] Véase https://www.ohchr.org/en/2021/07/use-spyware-surveil-journalists-and-human-rights-defendersstatement-un-high-commissioner.

pedido que, entre tanto, se suspenda el comercio de tecnología de vigilancia a fin de que los Estados puedan preparar un régimen de exportación y control, e impulsar unos marcos jurídicos que garanticen la privacidad[68]. Asimismo, la Relatora Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, la Relatora Especial sobre la situación de los defensores de los derechos humanos, el Relator Especial sobre los derechos a la libertad de reunión pacífica y de asociación, y miembros del Grupo de Trabajo sobre empresas y derechos humanos hicieron la siguiente declaración conjunta:

> En los últimos años hemos dado la voz de alarma en repetidas ocasiones sobre el peligro que supone para los derechos humanos la tecnología de vigilancia. Una vez más, instamos a la comunidad internacional a que elabore un marco regulador sólido para prevenir, mitigar y reparar los efectos negativos sobre los derechos humanos de la tecnología de vigilancia y, entre tanto, a que adopte una moratoria sobre su venta y transferencia[69].

En su informe de 2022 relativo al derecho a la privacidad en la era digital, el ACNUDH reiteró su apoyo a una moratoria provisional[70]. En abril de 2022, Costa Rica se convirtió en el primer Estado en sumarse al llamado a una moratoria sobre el comercio de tecnología de programas espía[71]; por otro lado, una amplia coalición de la sociedad civil reiteró la petición de una moratoria en la reunión del Foro Económico Mundial, celebrada en Davos (Suiza) en mayo de 2022[72].

49. Teniendo en cuenta la profunda preocupación que suscitan estas tecnologías y la cobertura que les dan el discurso y las prácticas contemporáneas de lucha contra el terrorismo, la Relatora Especial está de acuerdo con los llamamientos a que se suspendan las transferencias de este tipo de tecnología. No descarta que los Estados lleguen a la conclusión de que está justificada la prohibición permanente de los programas espía, pero secunda el llamamiento de la Alta Comisionada para que se investigue y se trabaje para elaborar un sistema regulador de la venta, el uso y la transferencia de tecnología de programas espía que respete los derechos humanos, ya sea como precursor de la prohibición o como medio de garantizar la protección de los derechos humanos sin necesidad de prohibición. El documento de posición de la Relatora Especial ofrece una propuesta sólida y novedosa de regulación internacional del comercio de programas espía con el fin de reducir al mínimo los riesgos para los derechos humanos.

50. Por último, la Relatora Especial subraya la necesidad de una supervisión independiente de la vigilancia y la recopilación de datos por motivos de seguridad nacional o lucha antiterrorista[73]. Observando que los organismos de inteligencia están impulsando y adaptando el cambio tecnológico y desplegando una avalancha de nuevas tecnologías, como el aprendizaje automático, para operaciones automatizadas de redes informáticas ofensivas y de defensa, la Relatora Especial pide una inversión sustancial de los Estados en capacidad de supervisión de la inteligencia. La austeridad en la supervisión de la vigilancia no puede justificarse dada la evolución de la tecnología de vigilancia, ya que la legitimidad de la conducta ejecutiva depende de una supervisión eficaz, moderna y exhaustiva de los servicios de inteligencia[74]. La Relatora Especial insta a que, como práctica general, los órganos de supervisión tengan acceso directo a los sistemas operativos de los servicios de inteligencia[75] y a que se les permita controlar los datos almacenados para detectar errores de archivo. También deberían participar en las verificaciones de minimización de datos para asegurar la supervisión de los registros de auditoría de inteligencia y crear métodos que permitan

[68] Véase https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=27455&LangID=E.

[69] Véase https://www.ohchr.org/en/press-releases/2021/08/spyware-scandal-un-experts-call-moratorium-sale-life-threatening.

[70] A/HRC/51/17, párr. 19.

[71] Véase https://www.accessnow.org/press-release/costa-rica-primer-pais-moratoria-spyware/.

[72] Véase https://www.accessnow.org/spyware-davos-press-conference/.

[73] A/HRC/10/3, párrs. 25 a 78 y A/HRC/14/46.

[74] Véase Kilian Vieth y Thorsten Wetzling, “Data-driven intelligence oversight: recommendations for a system update”, Stiftung Neue Verantwortung, 2019, pág. 9.

[75] Esto es esencial para llevar a cabo verificaciones aleatorias, inspecciones sin previo aviso y controles (semi)automatizados del tratamiento de datos por parte de los organismos de inteligencia.

supervisar si la detección de patrones sistemáticos muestra un alto solapamiento con el uso ilegal e inadecuado de las bases de datos de inteligencia. Por último, subraya que es urgente llevar a cabo una revisión de la cooperación en materia de inteligencia que respete los derechos humanos[76], lo que requerirá una selección coherente de la inteligencia transferida mediante métodos como las alertas de intercambio de datos a los órganos de supervisión, la revisión coherente de los archivos de registro, la supervisión de los archivos eliminados y una moratoria del intercambio de inteligencia con organismos de referencia que hayan sido considerados implicados en un cuadro persistente de violaciones de los derechos humanos[77].

E. Efectos del terrorismo: víctimas

51. En su resolución 42/18, el Consejo de Derechos Humanos invitó a la Relatora Especial a que reflexionara sobre los efectos negativos del terrorismo. En el informe que presentó al Consejo en 2021, la Relatora Especial analizó los parámetros jurídicos de los efectos del terrorismo a través de un marco de derechos humanos[78]. En ese informe, presentó información actualizada exhaustiva de las obligaciones de los Estados en materia de derechos humanos para con las víctimas del terrorismo, instando a los Estados a adoptar un enfoque de derechos humanos y a emprender medidas de protección, investigación, reparación, participación y conmemoración de las víctimas del terrorismo que respeten los derechos humanos y no sean discriminatorias[79].

52. La Relatora Especial aprovecha la oportunidad para tratar otros dos asuntos: las necesidades y derechos singulares de los niños víctimas del terrorismo y la necesidad de que los Estados adopten una legislación que respete los derechos humanos para proteger los derechos humanos de las víctimas del terrorismo.

53. Recalca los efectos duraderos del terrorismo en la vida de los niños, pone de relieve la obligación de los Estados de regirse por la Convención sobre los Derechos del Niño al tomar medidas respecto a los derechos de los niños víctimas y destaca que el interés superior del niño debe ser el criterio primordial de toda acción que se emprenda para atender a los niños víctimas del terrorismo. Señala que las medidas centradas en el niño y con perspectiva de género para tratar los traumas de los niños víctimas son esenciales y en muchos Estados están poco desarrolladas. Hay que centrarse en la resiliencia, pero también en el derecho a una atención de la salud y psicológica y una educación adaptadas a los niños, como vías que permiten y sostienen su recuperación a largo plazo.

54. La Relatora Especial expresa preocupación por los niños víctimas del Dáesh en el Iraq y la República Árabe Siria, miles de los cuales están detenidos arbitrariamente en los campamentos de Al-Hawl y Roj, en el norte de la República Árabe Siria. Subraya que los niños detenidos en esos campamentos deben ser tratados ante todo como víctimas del terrorismo, en consonancia con la Convención sobre los Derechos del Niño, la resolución 2427 (2018) del Consejo de Seguridad y la resolución 60/1 de la Asamblea General. A esos niños se les ha negado todo derecho que pueda contemplar la ley a vivir una infancia digna y protegida. Está especialmente alarmada por la situación de los niños y adolescentes varones detenidos por “asociación” en las denominadas instalaciones de rehabilitación, en condiciones que, a su juicio, cumplen los criterios para considerarse tortura y trato inhumano y degradante según el derecho internacional. La Relatora Especial afirma inequívocamente que los Estados no pueden escoger sus víctimas preferidas del terrorismo, y que negar la protección de víctimas a unos niños que han sido tratados de manera tan brutal por un grupo considerado como terrorista socava el principio de igualdad, fundamental para la protección de todas las víctimas del terrorismo sin discriminación. Recalca que, para proteger a estas

[76] La Relatora Especial destaca la gran dificultad que plantea en cuanto a los derechos humanos el hecho de que, una vez que los organismos de inteligencia comparten datos con asociados extranjeros, pierden el control sobre el uso futuro que se haga de esos datos.

[77] Hace notar las buenas prácticas de los órganos de supervisión de los servicios de inteligencia de Dinamarca y Suecia.

[78] A/HRC/46/36, párrs. 32 a 38.

[79] Véanse los Principios y Directrices sobre los Niños Asociados a Fuerzas Armadas o Grupos Armados (Principios de París) y la resolución 1314 (2000) del Consejo de Seguridad.

víctimas de los efectos del terrorismo y de la brutalidad que supone la detención indefinida y arbitraria, debe emprenderse urgentemente una repatriación respetuosa con los derechos humanos.

55. Por último, la Relatora Especial se refiere a la regulación nacional del terrorismo. Encomia las disposiciones legislativas modelo que sirven para apoyar las necesidades y proteger los derechos de las víctimas del terrorismo, elaboradas conjuntamente por la Unión Interparlamentaria, la Oficina de las Naciones Unidas contra la Droga y el Delito y la Oficina de Lucha contra el Terrorismo a las que tuvo el placer de proporcionar asistencia técnica y aportaciones[80]. Insta a los Estados a que adopten leyes nacionales que respeten los derechos humanos para proteger plenamente y por igual los derechos de todas las víctimas, incluidas las víctimas del terrorismo.

III. Recomendaciones

A. Estados

56. **La Relatora Especial recomienda que los Estados:**

a) Aprueben leyes nacionales amplias que protejan los derechos individuales y colectivos al recopilar datos por motivos de seguridad nacional, lucha contra el terrorismo, extremismo violento o extremismo;

b) Velen por que, en sus políticas y procedimientos para el uso de drones armados, tanto en un contexto de lucha contra el terrorismo y de conflicto como en otros contextos, incluso cuando actúen fuera de su territorio, observen estrictamente las normas establecidas del derecho internacional, el derecho internacional humanitario y el derecho internacional de los derechos humanos (según proceda), y que el uso de drones armados en el plano nacional esté sujeto a sólidos mecanismos de supervisión en plena conformidad con el derecho de los derechos humanos, aplicándose dicha supervisión con un criterio neutral desde el punto de vista tecnológico a todos los avances en la tecnología de los drones;

c) Aprueben leyes nacionales amplias que protejan adecuadamente el derecho a la privacidad como derecho de entrada que habilita y sustenta la protección de otros derechos humanos fundamentales, incluidos los derechos inderogables. Esto abarca legislación amplia sobre protección de datos;

d) Establezcan y apoyen una supervisión independiente y dotada de los recursos adecuados de las nuevas tecnologías en contextos de seguridad y lucha contra el terrorismo, incluida la creación de órganos independientes de supervisión de la privacidad de los datos. Paralelamente, los Estados deben garantizar que los órganos de supervisión de los servicios de inteligencia cuenten con recursos suficientes y la competencia tecnológica adecuada para hacer frente al uso expansivo de la tecnología por parte de las entidades de inteligencia, lo que abarca el acceso directo a los sistemas operativos de los servicios de inteligencia, el acceso a los datos almacenados, la supervisión de los registros de auditoría de los servicios de inteligencia, así como el establecimiento de mecanismos de supervisión de la cooperación en materia de inteligencia, como se expone en el presente informe;

e) Establezcan moratorias a la cooperación transfronteriza deficiente en materia de derechos humanos que facilite la transferencia de tecnologías de alto riesgo a Estados con un historial de violaciones de los derechos humanos de malo a crónico;

f) Proporcionen vías de recurso adecuadas y accesibles a las personas cuyos datos personales se hayan manejado o utilizado de forma indebida en contextos de lucha contra el terrorismo o de prevención y lucha contra el extremismo violento;

[80] Véase https://www.unodc.org/documents/terrorism/Website2021/220204_model_legislative_provisions.pdf.

g) Adopten medidas legislativas prácticas de protección frente a los abusos contra los derechos humanos por parte de las empresas del sector tecnológico;

h) Se comprometan a que el Equipo Especial del Pacto Mundial de Coordinación de la Lucha Antiterrorista de las Naciones Unidas y la Oficina de Lucha contra el Terrorismo se sometan a supervisión independiente.

57. **La Relatora Especial pide también que:**

a) Se revisen los proyectos de legislación de la Unión Europea en materia de IA para eliminar las exclusiones por motivos de seguridad nacional;

b) El proceso de elaboración del "borrador cero" del Consejo de Europa de un convenio sobre AI sea más transparente, inclusivo y abierto;

c) Como recomendó la Alta Comisionada en su informe, los Estados adopten regímenes rigurosos de control de las exportaciones para el comercio transfronterizo de tecnologías de vigilancia, con el fin de impedir la venta de dichas tecnologías cuando exista el riesgo de que estas puedan utilizarse para violar los derechos humanos, en particular para perseguir a defensores de los derechos humanos o periodistas[81].

d) Impongan una moratoria del uso de la tecnología de reconocimiento biométrico a distancia en los espacios públicos, al menos hasta que las autoridades responsables puedan demostrar el cumplimiento de las normas de privacidad y protección de datos, así como la ausencia de problemas significativos de precisión y de efectos discriminatorios, y hasta que se apliquen todas las recomendaciones formuladas en el párrafo 53 j) del informe[82] del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión[83].

B. Recomendaciones específicas para las Naciones Unidas

58. **La Relatora Especial recomienda que:**

a) Todas las entidades de las Naciones Unidas, la Oficina de Lucha contra el Terrorismo y, en particular, la Dirección Ejecutiva del Comité contra el Terrorismo aborden de forma completa y práctica las consecuencias para los derechos humanos de proporcionar fomento de la capacidad y asistencia técnica en el ámbito de las nuevas tecnologías —incluidas la IA, la biometría y las herramientas de gestión de fronteras— a Estados que tienen un historial demostrado de violaciones de los derechos humanos en relación con la seguridad y la lucha contra el terrorismo. Deben establecerse protocolos tanto de moratoria como de suspensión sobre el fomento de la capacidad y la asistencia técnica en el uso de tecnologías de alto riesgo, en consonancia con los principios y los marcos de apoyo de la política de diligencia debida en materia de derechos humanos;

b) Todas las entidades de las Naciones Unidas que participan en la programación en esas esferas establezcan matrices de riesgo específicas, protocolos de diligencia debida y capacidades de evaluación que sean oportunas, flexibles y se comprometan a cumplir el principio de no hacer daño. Esta medida es fundamental debido al alto riesgo que entrañan estas tecnologías y la elevada implicación de actores que no responden a la definición de fuerzas de seguridad del Estado en la política de diligencia debida en materia de derechos humanos;

c) El Secretario General inicie el proceso de inspección y evaluación internas o una auditoría externa independiente del Programa de Lucha contra los Viajes de Terroristas para velar por la integridad de sus prácticas y transferencias de tecnología en materia de derechos humanos, protección de datos y estado de derecho.

[81] A/HRC/41/35, párr. 49, y A/HRC/44/24, párr. 40. En estos informes, el Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión y la Alta Comisionada pedían una moratoria de la concesión de licencias para la exportación de tecnologías de vigilancia.

[82] A/HRC/44/24.

[83] A/HRC/48/31, párr. 59 d).

C. Empresas

59. **La Relatora Especial pone de relieve que:**

a) Las empresas de los sectores de las nuevas tecnologías deben llevar a cabo sus operaciones práctica y públicamente guiándose por el respeto al derecho internacional de los derechos humanos y actuar con la debida diligencia para evitar repercusiones negativas sobre las personas y las comunidades, incluso a través del marco para "proteger, respetar y remediar" establecido en los Principios Rectores sobre las Empresas y los Derechos Humanos[84]**;**

b) Las empresas del sector de las nuevas tecnologías deben llevar a cabo una exhaustiva diligencia debida en materia de derechos humanos, que implica realizar evaluaciones de riesgos de las repercusiones reales y potenciales, tanto directas como indirectas, sobre los derechos humanos durante todas las fases de sus operaciones;

c) Las empresas que se dedican a desarrollar, usar y transferir nuevas tecnologías de alto riesgo deben regirse por una regulación y supervisión más estrictas por parte de los órganos legislativos, los tribunales y la regulación internacional, y debe haber importantes sanciones económicas y administrativas para las empresas que no adopten prácticas adecuadas de diligencia debida.

[84] Véase https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_sp.pdf.

Annex

Draft Proposed State Commitments with Respect to the International Trade in Spyware

1. The current response to the challenge posed to human rights by the extremely powerful tools of the contemporary spyware industry is fractured and inadequate. Direct approaches to the voluntary responsibility of corporations developing and selling the technology rely upon the UN Guiding Principles on Business and Human Rights, the effectiveness of which is undermined by the absence of a binding enforcement arm. Domestic private law doctrines form an inconsistent patchwork, with ample room for argument about degrees of responsibility along transnational production chains, how human rights harms equate to (or diverge from) traditional models of physical harm, and how relationships between private entities and foreign sovereign entities ought to be dealt with. They also necessitate victims of unlawful surveillance having the knowledge and the means to use litigation to hold private companies to account. At the same time the export control system was developed for the radically different context of conventional arms. It grants exporting States generous latitude in their decision-making, providing the conditions for confusion, inconsistency, and arbitrage between jurisdictions.

2. All of this means that there is no obvious mechanism for accountability if corporations fail to advert to the harms to which their spyware technology may cause or contribute, and no clear deterrent to prevent producers from developing and trading in such technology without concern for its potential impacts.

3. As a result, the way forward for regulation of the spyware trade requires a novel approach which avoids the gaps in the existing patchwork of purported oversight and accountability methods.

4. A human rights analysis of the use of spyware in the counter-terrorism context suggests that spyware technology must at a minimum: (a) allow for users to specifically target certain data and metadata, rather than automatically monitor and record all data and metadata; (b) avoid automatically accessing data relating to contacts of targeted individuals, unless users specifically require that additional information for investigative purposes; and, in any event, (c) create an indelible, permanent, and uneditable auditable record of what actions have been taken by the user of the spyware, including any interferences/modifications of data/metadata, when those occurred, and by whom they were effected so that the use of the tool can be verified, and its human rights compliance assessed after the fact by judicial authorities. Part of that indelible and uneditable record must be some form of identifier or watermark such that judicial authorities overseeing complaints may verify the producer of spyware alleged to have been used against a victim and the customer to which that spyware was originally supplied and, from such source, can compel disclosure of the auditable record such that the legality of any use complained of can be adequately reviewed. Spyware which fails to display such features cannot, however otherwise tightly regulated, be capable of human rights compliance.

5. It is therefore recommended that States adopt commitments substantively equivalent to the following draft proposals:

> *'Each State party shall, within two years from the date of their signature, give binding domestic effect to the following obligations (whether through the enaction of domestic legislation or such other steps (if any) as are required under its national law):*
>
> 1. Companies domiciled within their jurisdiction are prohibited from manufacturing or offering for sale or other provision spyware technology which fails to display the following cumulative characteristics:
>
> (a) Not automatically granting access to all data and/or metadata once the spyware infiltrates a network, computer, or device, and instead providing that the user must positively select the types of data and/or metadata for monitoring;

(b) Not automatically granting access to any data and/or metadata regarding contacts of the target network, computer, or device, and instead providing that the user must positively select any contacts for monitoring;

(c) Providing in all cases of use of the spyware that there is created an indelible, permanent, and uneditable auditable record of what actions have been taken by the user of the spyware, including any interferences/modifications of data/metadata, when those occurred, and by whom they were affected. This record must include a record of the producer and customer for the spyware technology, so that judicial authorities may properly be able to identify the producer and purchase of spyware used in any particular instance;

2. Companies domiciled within their jurisdiction are made subject to a binding obligation to undertake a human rights due diligence exercise upon the purchasers, and, if different, the reasonably foreseeable end users, of spyware technology sold. Such human rights due diligence shall be proportionate to the risk of the technology being used by purchasers, or reasonably foreseeable end users, in breach of international human rights law;

3. As a separate and independent obligation, companies domiciled within their jurisdiction are made subject to a binding obligation only to sell spyware technology in circumstances where they can prove that there is no tangible risk of the technology being used by purchasers, or reasonably foreseeable end users, in breach of international human rights law;

4. For the avoidance of doubt, while the fact that such companies have obtained guarantees or assurances of compliance with international human rights law from purchasers, and/or, if different, the reasonably foreseeable end users, may be taken into account in the due diligence exercise and in the companies' assessment of the real risk of breach, the mere fact of such guarantees or assurances will not, of itself, be sufficient to demonstrate compliance with their obligations set out above;

5. As a separate and independent obligation, companies domiciled within their jurisdiction are subject to a binding obligation not to sell spyware to the agencies of any State which is not itself a signatory of this treaty;

6. Breaches of the obligations set out above are to be actionable in the ordinary domestic courts of the State on the application of persons including but not limited to persons capable of demonstrating that they are likely (subject to an appropriate evidential burden) to have been victims of breaches of international human rights law connected with the use of that companies' technology; and

7. In the event that a court determines that a breach has occurred, the persons bringing actions in respect of the same are entitled to such remedies as are available in domestic law adequately to compensate them for the violations of their international human rights which are found to have occurred.