Naciones Unidas S/2025/22

Consejo de Seguridad

Distr. general
10 de enero de 2025
Español
Original: inglés

Carta de fecha 9 de enero de 2025 dirigida a la Presidencia del Consejo de Seguridad por la Presidencia del Consejo de Seguridad en ausencia de una Presidencia del Comité del Consejo de Seguridad establecido en virtud de la resolución 1373 (2001) relativa a la lucha contra el terrorismo

En nombre del Comité del Consejo de Seguridad establecido en virtud de la resolución 1373 (2001) relativa a la lucha contra el terrorismo, tengo el honor de referirme a los principios rectores no vinculantes sobre la prevención, la detección y la interrupción del uso de tecnologías financieras nuevas y emergentes con fines terroristas (véase el anexo), que se conocerán con el nombre de “Principios Rectores de Argelia”, preparados de conformidad con la Declaración de Delhi sobre la lucha contra el uso de las tecnologías nuevas y emergentes con fines terroristas, en la que el Comité decidió elaborar un conjunto de principios rectores no vinculantes con el fin de ayudar a los Estados Miembros a contrarrestar la amenaza que supone el uso de las tecnologías nuevas y emergentes con fines terroristas.

Le agradecería que la presente carta y su anexo se publicaran como documento del Consejo de Seguridad.

(*Firmado*) Amar **Bendjama**
Presidente del Consejo de Seguridad en ausencia
de una Presidencia del Comité del Consejo de Seguridad
establecido en virtud de la resolución 1373 (2001)
relativa a la lucha contra el terrorismo

Anexo

Principios rectores no vinculantes para los Estados Miembros sobre la prevención, la detección y la interrupción del uso de tecnologías financieras nuevas y emergentes con fines terroristas[1]

1. Las tecnologías nuevas y emergentes ofrecen posibles beneficios de gran alcance en múltiples ámbitos, como la salud pública, el control de las fronteras, la aplicación de la ley, el transporte, la asistencia humanitaria y los sistemas de comunicación.

2. Aunque aportan muchos beneficios a la sociedad, las tecnologías nuevas y emergentes están siendo utilizadas con fines terroristas por el EIIL (Dáesh), Al-Qaida, sus grupos afiliados, otras organizaciones terroristas y sus seguidores. Los Estados Miembros ya están lidiando con la amenaza considerable y cada vez mayor que plantea el empleo de las tecnologías nuevas y emergentes para facilitar una amplia gama de actividades terroristas.

3. Consciente de la creciente amenaza que plantea el uso indebido de las tecnologías nuevas y emergentes, así como de las múltiples formas beneficiosas en que se pueden usar las tecnologías para contrarrestar el terrorismo, el Comité contra el Terrorismo celebró en la India una sesión especial sobre la lucha contra el uso de las tecnologías nuevas y emergentes con fines terroristas y aprobó la Declaración de Delhi el 29 de octubre de 2022.

4. El Comité contra el Terrorismo también expresó su intención de elaborar, con el apoyo de la Dirección Ejecutiva del Comité contra el Terrorismo, un conjunto de principios rectores no vinculantes con el fin de ayudar a los Estados Miembros a contrarrestar la amenaza que plantea el uso de las tecnologías nuevas y emergentes con fines terroristas, entre otras cosas recopilando buenas prácticas sobre las oportunidades que ofrece ese mismo conjunto de tecnologías para contrarrestar la amenaza, en consonancia con el derecho internacional de los derechos humanos y el derecho internacional humanitario. Para facilitar la elaboración de los principios rectores, la Dirección Ejecutiva, en nombre del Comité, emprendió un amplio proceso de consultas sobre cada uno de los tres temas con expertos de organismos de las Naciones Unidas y organizaciones internacionales y regionales asociadas, así como con diversas partes interesadas de la Red Mundial de Investigación sobre la Lucha Antiterrorista de la Dirección Ejecutiva, entre ellas el sector privado, el mundo académico y la sociedad civil.

5. El Consejo de Seguridad ha reafirmado que los Estados Miembros deben velar por que las medidas que adopten para combatir la amenaza que plantean las tecnologías nuevas y emergentes usadas con fines terroristas sean compatibles con todas sus obligaciones en virtud del derecho internacional, en particular el derecho internacional de los derechos humanos, el derecho internacional de los refugiados y el derecho internacional humanitario; ha recalcado que las medidas antiterroristas efectivas y el respeto de los derechos humanos, las libertades fundamentales y el estado de derecho se complementan y refuerzan mutuamente, y son esenciales para el éxito de la lucha antiterrorista; y ha observado la importancia de integrar el género como cuestión transversal, en consonancia con su resolución 2617 (2021).

[1] La finalidad y el objetivo de estos principios rectores no vinculantes es ayudar a los Estados Miembros a mejorar las medidas nacionales y reforzar la cooperación internacional; no se pretende con ellos imponer ninguna obligación jurídica a los Estados.

6. El presente conjunto de principios rectores no vinculantes ha sido elaborado por el Comité contra el Terrorismo y constituye un esfuerzo por ayudar a los Estados Miembros a contrarrestar el uso de las tecnologías nuevas y emergentes con fines terroristas de manera compatible con el derecho internacional.

7. Los siguientes principios rectores tienen por objeto complementar otros materiales a fin de guiar a los Estados Miembros y la labor del Comité contra el Terrorismo y la Dirección Ejecutiva del Comité contra el Terrorismo por ayudar a los Estados a aplicar las resoluciones del Consejo de Seguridad 1373 (2001), 1624 (2005), 2178 (2014), 2370 (2017), 2396 (2017), 2462 (2019) y 2617 (2021) y otros documentos pertinentes del Consejo sobre la lucha contra el terrorismo[2]. Muchos de los principios rectores expuestos en el presente documento se basan en la labor y las buenas prácticas recomendadas del Consejo de Seguridad y la Asamblea General, las organizaciones asociadas de las Naciones Unidas y otras partes interesadas clave, como el Grupo de Acción Financiera.

Amenazas que plantea el uso de tecnologías financieras nuevas y emergentes con fines terroristas

8. Como reconoció el Consejo de Seguridad, las innovaciones en tecnologías financieras pueden crear considerables oportunidades económicas[3], pero también corren el riesgo de ser utilizadas indebidamente, incluso con fines terroristas[4]. Desde entonces, la magnitud creciente del uso indebido ha sido un aspecto destacado en varios informes de las Naciones Unidas y el Grupo de Acción Financiera y los organismos regionales al estilo del Grupo de Acción Financiera, así como por miembros de la Red Mundial de Investigación de la Dirección Ejecutiva sobre la Lucha Antiterrorista y asociados del sector privado[5].

---

[2] Entre ellos, los principios rectores sobre los combatientes terroristas extranjeros (S/2015/939); la adición a los principios rectores sobre los combatientes terroristas extranjeros (2018) (S/2018/1177); la guía técnica para la aplicación de la resolución 1373 (2001) del Consejo de Seguridad y otras resoluciones pertinentes (S/2019/998); el documento marco para las visitas del Comité contra el Terrorismo a los Estados Miembros (S/2020/731); y el estudio mundial sobre la aplicación de la resolución 1373 (2001) por los Estados Miembros, publicado en 2009, 2011, 2016 y 2021 (S/2009/620, S/2011/463, S/2016/49 y S/2021/972).

[3] Resolución 2462 (2019) del Consejo de Seguridad, décimo párrafo del preámbulo; véase también Grupo de Acción Financiera, *Opportunities and Challenges of New Technologies for AML/CFT* (París, 2021), disponible en https://www.fatf-gafi.org/en/publications/Digitaltransformation/Opportunities-challenges-new-technologies-for-aml-cft.html.

[4] Resolución 2462 (2019) del Consejo de Seguridad, décimo párrafo del preámbulo; también reiterado en la resolución 2617 (2021), vigésimo quinto párrafo del preámbulo.

[5] Para consultar más detalles, véanse el 18º informe del Secretario General sobre la amenaza que plantea el EIIL (Dáesh) para la paz y la seguridad internacionales y la gama de actividades que realizan las Naciones Unidas en apoyo de los Estados Miembros para combatir la amenaza (S/2024/117), párr. 14; el 34º informe del Equipo de Apoyo Analítico y Vigilancia de las Sanciones presentado de conformidad con la resolución 2734 (2024), relativa al EIIL (Dáesh), Al-Qaida y las personas y entidades asociadas (S/2024/556), párrs. 94 a 97; Dirección Ejecutiva del Comité contra el Terrorismo, Resumen informativo sobre las tendencias más recientes en el uso de criptomonedas por los grupos terroristas afiliados con el Dáesh (EIIL)/Al-Qaida y sus seguidores, 4 de marzo de 2024 (véase https://www.un.org/securitycouncil/ctc/news/cted-hosts-insight-briefing-%E2%80%9Clatest-trends-use-cryptocurrency-terrorist-groups-and-their); Grupo de Acción Financiera, “Public Statement on the Financing of ISIL, Al Qaeda and Affiliates”, 21 de octubre de 2021, y actualizaciones posteriores no públicas; y Grupo de Asia y el Pacífico sobre Blanqueo de Dinero, *APG Yearly Typologies Report 2021* (Sídney, 2021), disponible en www.apgml.org/includes/handlers/get-document.ashx?d=6bfd011b-8edd-40f4-93e4-f219e1c6d73e. Véanse también, por ejemplo, Elliptic, *Preventing Financial Crime in Cryptoassets: Typologies Report 2022*, disponible en www.elliptic.co/resources/typologies-report-2022; TRM, *Illicit Crypto Ecosystem Report* (2023), disponible en

9. La magnitud del uso indebido y sus tipos varían notablemente en función del contexto regional y económico, los medios disponibles y los objetivos que se fijen los terroristas en cuanto a sus fuentes y métodos de financiación. Una tendencia cada vez más extendida en la financiación del terrorismo es el uso mixto de formas antiguas y nuevas de recaudar y mover fondos[6], el cual básicamente combina las dificultades y complejidades asociadas con cada método, desde la detección del transporte transfronterizo físico de dinero en efectivo hasta el rastreo de complicadas transacciones virtuales. Por tanto, los Estados deberían adoptar un enfoque amplio basado en los riesgos para luchar contra la financiación del terrorismo, de modo que no desestimen protecciones en lo tocante a los métodos y los canales utilizados por los terroristas. Un marco basado en riesgos, actualizado y eficiente de lucha contra el blanqueo de dinero y la financiación del terrorismo, de conformidad con el derecho internacional, es esencial para mitigar numerosas vulnerabilidades de la financiación del terrorismo.

10. Algunos ejemplos de los métodos con que se recaudan fondos con fines terroristas usando tecnologías nuevas y emergentes son el uso indebido de los servicios de redes sociales (para recabar donaciones mediante métodos de pago tradicionales), los servicios de hospedaje de contenido, la venta de productos en línea y las plataformas de financiación colectiva[7]. En su informe más reciente, el Grupo de Acción Financiera determinó que, entre todas las formas diferentes de financiación colectiva, la basada en donaciones era la que tenía más probabilidades de ser explotada para la financiación del terrorismo[8]. Las cuatro tipologías principales de uso indebido de la financiación colectiva para financiar el terrorismo que figuran en el informe son el uso indebido de causas humanitarias, benéficas o sin fines de lucro; el uso de plataformas o sitios web de financiación colectiva específicos; el uso de plataformas de medios sociales y aplicaciones de mensajería; y la interacción de la financiación colectiva con activos virtuales. Sin embargo, la supervisión regulatoria del sector de la financiación colectiva en el plano mundial sigue estando fragmentada, entre otras cosas en cuanto al cumplimiento de las reglas de lucha contra el blanqueo de dinero y la financiación del terrorismo[9]. Pese a que los terroristas han usado en repetidas ocasiones plataformas de medios sociales y de financiación colectiva para actividades financieras, algunas plataformas y aplicaciones de chat tienen dificultades para adaptarse a los sistemas de autovigilancia y moderación de contenido a fin de lidiar con la financiación del terrorismo que se pueda estar produciendo a través de

www.trmlabs.com/illicit-crypto-ecosystem-report-2023; TRM, “Terrorist financing: six crypto-related trends to watch in 2023”, 16 de febrero de 2023, disponible en https://www.trmlabs.com/post/terrorist-financing-six-crypto-related-trends-to-watch-in-2023; y TRM, “TRM finds mounting evidence of crypto use by ISIS and its supporters in Asia”, 21 de julio de 2023, disponible en https://www.trmlabs.com/post/trm-finds-mounting-evidence-of-crypto-use-by-isis-and-its-supporters-in-asia.

[6] Esta fue también una conclusión importante de la última reunión conjunta de expertos del Grupo de Acción Financiera y del taller conjunto del Grupo de Acción Financiera y la Oficina de las Naciones Unidas contra la Droga y el Delito sobre la financiación del terrorismo mediante la *hawala* y servicios similares (Nueva Delhi, abril de 2023).

[7] S/2024/556, párr. 94; véanse las fuentes de referencia citadas en www.un.org/securitycouncil/ctc/news/cted%E2%80%99s-tech-sessions-highlights-%E2%80%9Cthreats-and-opportunities-related-new-payment-technologies-0.

[8] Grupo de Acción Financiera, *Crowdfunding for Terrorism Financing* (París, 2023), párr. 38, disponible en https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Crowdfunding-Terrorism-Financing.pdf.coredownload.inline.pdf.

[9] *Ibid.*, párrs. 27, 28 y 30. En el informe, se señala que en la red mundial del Grupo de Acción Financiera solo hay cuatro jurisdicciones que regulen la financiación colectiva tanto de inversión como basada en donaciones en el contexto de sus marcos de lucha contra el blanqueo de dinero y la financiación del terrorismo.

sus plataformas[10]. También hay otras oportunidades de recaudación de fondos que se pueden facilitar por medio de tecnologías en línea y se usan indebidamente con fines terroristas, como la función de “super chat” o las marcas que se anuncian y ofrecen monetización junto a contenido de carácter terrorista, ya que las tendencias y las tácticas no dejan de evolucionar.

11. Los investigadores, las autoridades nacionales y las instancias normativas multilaterales indican que, si bien los sistemas en efectivo o tipo hawala siguen siendo los métodos más utilizados para mover dinero con fines terroristas (en la mayoría de las transferencias relacionadas con la financiación del terrorismo), también ha aumentado su uso en combinación con las tecnologías y los métodos de pago nuevos. Los sistemas de pago móvil, los activos virtuales y las bolsas y billeteras en línea se han usado de manera indebida con fines terroristas y se prevé que este uso se vuelva aún más generalizado y significativo[11]. El rastro del dinero de estos métodos, con frecuencia complejo, plantea dificultades a los investigadores financieros y a las instituciones financieras con las que interactúan. Algunos activos virtuales permiten las transferencias de fondos transfronterizas entre pares con seudónimos, que pueden realizarse sin la intervención de un proveedor de servicios de activos virtuales[12]. Estos riesgos se ven agravados por el hecho de que algunos países sigan sin poner en práctica los estándares del Grupo de Acción Financiera correspondientes a los activos virtuales y los proveedores de servicios de activos virtuales, en particular la recomendación 15 y la nota interpretativa correspondiente. La financiación descentralizada y las billeteras no alojadas, pese a ser un subgrupo del ecosistema más amplio de activos virtuales, entrañan riesgos de financiación del terrorismo y otros delitos financieros. Algunas jurisdicciones han informado sobre las dificultades para mitigar estos riesgos.

12. El Consejo de Seguridad ha exhortado a todos los Estados Miembros a que evalúen y afronten los posibles riesgos asociados con los activos virtuales y, según proceda, los riesgos que plantean los nuevos instrumentos financieros, incluidas las plataformas de financiación colectiva, que se pueden utilizar indebidamente con el propósito de financiar el terrorismo, y a que adopten medidas para asegurar que los proveedores de activos de ese tipo cumplan sus obligaciones relativas a la lucha contra el blanqueo de dinero y la financiación del terrorismo[13].

13. Además, el Consejo de Seguridad ha instado encarecidamente a todos los Estados a que pongan en práctica los estándares internacionales amplios incorporados en la versión revisada de las Cuarenta Recomendaciones del Grupo de Acción Financiera sobre la Lucha Contra el Blanqueo de Dinero y la Financiación del Terrorismo y la Proliferación[14]. La recomendación 15 sobre nuevas tecnologías (revisada en 2018 y complementada con una nota interpretativa en 2019) indica que los países y las instituciones financieras deben identificar y evaluar los riesgos de blanqueo de dinero o financiación del terrorismo que pudieran surgir con respecto a:

[10] Por ejemplo, en virtud del Reglamento de Servicios Digitales de la Unión Europea, las grandes plataformas deberán realizar sus propias evaluaciones de riesgos y retirar el contenido ilícito cuando reciban una notificación de las autoridades, pero no se hace referencia explícita a la financiación del terrorismo como forma de contenido ilícito. Como se recalcó en las reuniones de expertos mencionadas, en la actualidad, GoFundMe es la única plataforma de financiación colectiva que cuenta con disposiciones específicas sobre la financiación del terrorismo en sus términos de referencia.

[11] S/2024/556, párr. 95.

[12] Sobre el creciente uso por el EIIL y sus afiliados de criptomonedas de anonimato mejorado (también llamadas monedas de privacidad), en particular Monero, una criptomoneda que usa tecnologías criptográficas diseñadas para ocultar los detalles de las transacciones, véase *ibid.*, párrs. 96 y 97.

[13] Resolución 2462 (2019), párr. 20 d).

[14] *Ibid.*, párr. 4.

a) el desarrollo de nuevos productos y nuevas prácticas comerciales, incluyendo nuevos mecanismos de envío; y b) el uso de nuevas tecnologías o tecnologías en desarrollo para productos tanto nuevos como existentes. Para gestionar y mitigar los riesgos que surjan de los activos virtuales[15], los países deben tomar medidas para garantizar que los proveedores de servicios de activos virtuales estén regulados para propósitos de lucha contra el blanqueo de dinero y la financiación del terrorismo, y tengan licencia o registro y estén sujetos a sistemas efectivos para vigilar y asegurar el cumplimiento de las medidas relevantes requeridas en las recomendaciones del Grupo de Acción Financiera, o de lo contrario tendrán prohibido operar en el país[16]. En febrero de 2023, el Grupo de Acción Financiera aprobó una hoja de ruta para mejorar la puesta en práctica de la recomendación 15. Sin embargo, según el análisis hecho por el Grupo de Acción Financiera, a junio de 2024, en numerosas jurisdicciones no se logró avanzar lo suficiente en la puesta en práctica de los requisitos fundamentales del Grupo en relación con los activos virtuales y los proveedores de servicios de activos virtuales[17].

14. Asimismo, el Consejo de Seguridad ha pedido que se haga uso plenamente de las tecnologías financieras y regulatorias nuevas y emergentes para promover la inclusión financiera y contribuir a la aplicación efectiva de las medidas de lucha contra el blanqueo de dinero y la financiación del terrorismo, de conformidad con el derecho internacional. Efectivamente, y como destaca la labor del Grupo de Acción Financiera, las nuevas tecnologías también tienen potencial para hacer que las medidas de lucha contra el blanqueo de dinero y la financiación del terrorismo, tanto en el sector público como en el privado, sean más rápidas, baratas, transparentes e inclusivas, sin dejar de ser seguras[18]. Cuando se utiliza de manera responsable y proporcional, la tecnología puede facilitar la reunión, el procesamiento y el análisis

[15] Para obtener más información, véase Grupo de Acción Financiera, Focus on Virtual Assets, disponible en https://www.fatf-gafi.org/en/topics/virtual-assets.html.

[16] Para obtener más detalles, véanse Grupo de Acción Financiera, “Targeted update on implementation of the FATF standards on virtual assets and virtual asset service providers”, junio de 2024, págs. 4 y 5, disponible en https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2024.html; y Grupo de Acción Financiera, *Updated Guidance for a Risk-Based Approach: Virtual Assets and Virtual Asset Service Providers* (París, 2021), párrs. 31 a 43.

[17] Grupo de Acción Financiera, “Targeted update on implementation of the FATF standards on virtual assets and virtual asset service providers”. En el informe, el Grupo de Acción Financiera señala que, si bien la puesta en práctica de las regulaciones relativas a la lucha contra el blanqueo de dinero y la financiación del terrorismo ha avanzado en algunas jurisdicciones, a nivel mundial sigue rezagada. Varios Gobiernos no han tomado aún medidas significativas para regular el sector, y estos países deben dar prioridad a la puesta en práctica de los estándares del Grupo de Acción Financiera en su totalidad sin más dilación. Sobre la base de los 130 informes de evaluación mutua y de seguimiento publicados desde que se aprobó la versión revisada de la recomendación 15 en 2019, el 75 % de las jurisdicciones han cumplido solo parcialmente los requisitos del Grupo de Acción Financiera o no los han cumplido, porcentaje que es idéntico al de abril de 2023 (el 75 % de las jurisdicciones los cumplen parcialmente o no los cumplen, o 73 de 98) y registra una mejora insignificante. Véanse también Grupo de Acción Financiera, “Status of implementation of recommendation 15 by FATF members and jurisdictions with materially important VASP activity”, marzo de 2024, disponible en https://www.fatf-gafi.org/content/dam/fatf-gafi/publications/VACG-Table-Jurisdictions-2024.pdf.coredownload.pdf; y Dirección Ejecutiva del Comité contra el Terrorismo, “Thematic summary assessment of gaps in implementing key countering the financing of terrorism provisions of Security Council resolutions”, diciembre de 2022, págs. 16 a 18, disponible en www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/cted_2022_cft_gaps_assessment_final.pdf.

[18] Véase también Consejo de Estabilidad Financiera, “G20 roadmap for enhancing cross-border payments: priority actions for achieving the G20 targets”, 23 de febrero de 2023, disponible en https://www.fsb.org/2023/02/g20-roadmap-for-enhancing-cross-border-payments-priority-actions-for-achieving-the-g20-targets/.

de datos y ayudar a los agentes a detectar y gestionar los riesgos de financiación del terrorismo de manera más eficaz y oportuna[19].

15. Es importante también recordar que el Consejo de Seguridad exigió que "los Estados Miembros se cercioren de que todas las medidas que adopten para luchar contra el terrorismo, incluidas las medidas encaminadas a contrarrestar la financiación del terrorismo dispuestas en la presente resolución, estén en consonancia con las obligaciones que les incumben en virtud del derecho internacional, incluidos el derecho internacional humanitario, el derecho internacional de los derechos humanos y el derecho internacional de los refugiados"[20]. Además, el Consejo instó a los Estados a que, "cuando formulen y apliquen medidas de lucha contra la financiación del terrorismo, tengan en cuenta los efectos que pueden tener esas medidas en las actividades de carácter exclusivamente humanitario, incluidas las actividades médicas, que realicen agentes humanitarios imparciales de manera compatible con el derecho internacional humanitario"[21]. Al preparar y poner en práctica medidas para luchar contra la financiación del terrorismo, los Estados Miembros también deberían tener en cuenta las consecuencias inesperadas y las repercusiones en la actividad humanitaria y los derechos humanos, y en las actividades legítimas de las organizaciones sin fines de lucro y la sociedad civil.

16. Habida cuenta de la velocidad a la que avanzan las tecnologías financieras nuevas y emergentes, que hacen posible el movimiento transfronterizo de fondos al instante, antes de que el sistema regulatorio mundial haya aplicado controles y la obligación de notificar a las entidades en cuestión, los Estados Miembros deberían elaborar medidas para detectar, evaluar y contrarrestar las amenazas que conllevan. Hace falta aumentar el intercambio de información y prácticas en esta esfera entre las autoridades competentes, la sociedad civil, el mundo académico y el sector privado; reforzar la cooperación internacional y la asistencia judicial recíproca; mejorar la comprensión de los riesgos emergentes; analizar las oportunidades ofrecidas y los riesgos que plantean las tecnologías financieras modernas en el contexto de la lucha contra el terrorismo; y estudiar maneras de llegar a un enfoque más holístico a nivel mundial.

Principio rector no vinculante 1: mejorar la comprensión de los riesgos de financiación del terrorismo vinculados a las tecnologías financieras y los métodos de recaudación de fondos nuevos y emergentes

17. Comprender la naturaleza y el alcance de la amenaza sigue siendo el primer paso esencial para formular respuestas adecuadas, sobre todo teniendo en cuenta las posibles ventajas de estas tecnologías para luchar contra el terrorismo y su financiación. Las formas indebidas en que los agentes terroristas utilizan las nuevas tecnologías pueden variar notablemente en función de la proximidad y el alcance de

[19] Véase, por ejemplo, Grupo de Acción Financiera, *Opportunities and Challenges of New Technologies for AML/CFT*.

[20] Resolución 2462 (2019), párr. 6; véase también la resolución 2617 (2021), en la que el Consejo de Seguridad recordó la importancia de que se respetaran plenamente los derechos a la libertad de expresión y de asociación de las personas en la sociedad civil y la libertad de religión o de creencias y subrayó la importancia de adoptar medidas para contrarrestar la financiación del terrorismo eficaces y proporcionales de pertinencia para las organizaciones sin fines de lucro.

[21] Resolución 2462 (2019), párr. 24; véase también la resolución 2482 (2019), párr. 16, en la que se amplió este requisito a todas las medidas adoptadas para contrarrestar el terrorismo. Asimismo, determinadas transacciones financieras definidas en el párrafo 1 de la resolución 2664 (2022) necesarias para asegurar la entrega oportuna de asistencia humanitaria o apoyar la realización de otras actividades destinadas a atender las necesidades humanas básicas están permitidas en las situaciones a las que sean aplicables las sanciones financieras selectivas del Consejo de Seguridad, y no constituyen una violación de las medidas de congelación de activos (véase también la resolución 2761 (2024)).

la actividad terrorista, la disponibilidad de las tecnologías, las necesidades financieras de los terroristas y los contextos regional y económico. Centrarse en exceso en riesgos asociados con determinados tipos de productos o servicios nuevos e ignorar otros más tradicionales usados habitualmente para financiar el terrorismo[22] no es congruente con el enfoque basado en los riesgos. Por tanto, la comprensión de los riesgos debería basarse en una evaluación de las prácticas financieras de los terroristas en circunstancias dependientes del contexto para discernir cómo, cuándo y por qué los terroristas adoptan tecnologías nuevas y emergentes para financiar sus actividades. Las respuestas que se sustentan en riesgos *supuestos* de financiación del terrorismo, en lugar de en datos empíricos, suelen ser innecesarias y desproporcionadas respecto de las ventajas de las nuevas tecnologías financieras, entre otras su potencial de resolver la exclusión financiera, y corren el riesgo de contravenir el derecho internacional, incluido el derecho internacional de los derechos humanos.

18. A fin de analizar las amenazas, los riesgos y las vulnerabilidades relacionados con el uso de tecnologías financieras nuevas y emergentes con fines de financiación del terrorismo, los Estados Miembros deberían considerar lo siguiente:

a) Realizar evaluaciones nacionales de riesgos periódicas, inclusivas y con base empírica sobre la financiación del terrorismo que tomen en consideración el clima operacional y el contexto singulares de cada Estado, así como las tendencias mundiales y regionales de dicha financiación. A fin de mantenerse al día, deberían realizarse evaluaciones de riesgos exhaustivas de forma periódica (y complementarlas con evaluaciones de riesgos sectoriales, de ser necesarias);

b) Integrar en sus evaluaciones nacionales de riesgos un análisis de los riesgos de financiación del terrorismo relacionados con las tecnologías de pago y los métodos de recaudación de fondos nuevos y emergentes, y determinar cuáles son las vulnerabilidades de productos y servicios específicos, de manera compatible con la resolución 2462 (2019) y las recomendaciones del Grupo de Acción Financiera pertinentes;

c) Ampliar la investigación y el análisis de las amenazas pertinentes relativas a la financiación del terrorismo a la mayor variedad posible de grupos terroristas, incluidos los motivados por la xenofobia, el racismo y otras formas de intolerancia o en nombre de la religión o las creencias, y mantenerse al día de las tendencias regionales y mundiales[23], procurando también averiguar los métodos y los instrumentos de financiación utilizados por cada grupo;

d) Colaborar de manera proactiva con las contrapartes internacionales en jurisdicciones en las que se hayan detectado vínculos conocidos con la financiación del terrorismo;

e) Adoptar un enfoque multipartito, entre otras cosas interacciones e intercambios eficaces entre las autoridades nacionales competentes, el sector privado, la sociedad civil y el mundo académico, a fin de forjarse una imagen completa de los riesgos de financiación del terrorismo existentes y en evolución sobre la base de diversas experiencias y perspectivas y comprendiendo mejor las ventajas que reportan estas tecnologías y la magnitud de la amenaza y las repercusiones en

[22] Los terroristas siguen recaudando fondos por diversos medios, entre ellos la utilización indebida de empresas comerciales legítimas, la explotación de los recursos naturales, el uso indebido de organizaciones sin fines de lucro, las donaciones y el producto de actividades delictivas, entre ellas el secuestro para obtener rescate, la extorsión, la trata de personas, el tráfico ilícito de bienes culturales y el tráfico de drogas y de armas. Los fondos relacionados con la financiación del terrorismo siguen moviéndose por medio de instituciones financieras formales, sistemas informales y mensajeros de efectivo.

[23] Véase también S/2021/972, anexo, párr. 668.

diferentes categorías de sectores y poblaciones, entre ellas las comunidades locales, así como la realidad de cada región, a fin de facilitar la preparación de una respuesta adaptada y proporcionada;

f) Realizar evaluaciones con base empírica de los riesgos de financiación del terrorismo relacionados con los medios sociales, lo que incluye determinar cuáles son las funciones específicas que se usan para la integración con servicios de pago[24];

g) Consultar las metodologías actualizadas que publican las organizaciones multilaterales pertinentes para realizar evaluaciones nacionales de riesgos periódicas, inclusivas y con base empírica sobre la financiación del terrorismo y, de ser necesario, solicitar asistencia técnica para realizarlas;

h) Sensibilizar a todos los sectores y las partes interesadas pertinentes sobre las ventajas, los riesgos y las vulnerabilidades encontrados;

i) Adoptar medidas para velar por que las instituciones financieras realicen evaluaciones de riesgos propias antes de introducir nuevos productos o prácticas comerciales o de utilizar tecnologías nuevas o en desarrollo, y tomar las medidas adecuadas para gestionar y mitigar esos riesgos, como se indica en la recomendación 15 del Grupo de Acción Financiera.

Principio rector no vinculante 2: desarrollar y llevar a la práctica medidas de regulación, vigilancia y supervisión proporcionales y basadas en los riegos para prevenir el uso indebido de las nuevas tecnologías con fines de financiación del terrorismo

19. Como se señaló durante las consultas para la preparación de estos principios rectores no vinculantes, los Estados deberían revisar y readaptar, de forma constante y en función de las necesidades, sus marcos regulatorios vigentes a fin de asegurarse de que sean útiles, específicos y eficaces para hacer frente a las vulnerabilidades que conllevan las tecnologías financieras emergentes. Para lograrlo, las medidas de respuesta de los Estados deberían ser idóneas para ese fin, fundamentarse en una evaluación de riesgos con base empírica en lugar de en supuestas vulnerabilidades y ser acordes con el enfoque basado en los riesgos con arreglo a los estándares del Grupo de Acción Financiera. También deberían ser equilibradas en cuanto al potencial de las nuevas tecnologías financieras de aumentar la inclusión financiera como factor impulsor importante de diversos Objetivos de Desarrollo Sostenible, así como para innovar los pagos y los medios de efectuarlos de manera segura en situaciones de crisis. Como ha señalado el Grupo de Acción Financiera, “la tecnología financiera innovadora y otros productos financieros pueden apoyar las actividades de las [organizaciones sin fines de lucro], especialmente la entrega de ayuda a zonas de difícil acceso” y contribuir a mejorar la rastreabilidad de las transacciones financieras, “reduciendo así no solo el riesgo de desvío de fondos, sino también apoyando una pista de auditoría segura para la entrega de ayuda”[25]. Por el contrario, regular y supervisar de manera desproporcionadamente restrictiva las plataformas digitales de pago puede limitar sin necesidad los derechos humanos y obstaculizar la prestación de ayuda humanitaria por agentes humanitarios imparciales de manera compatible con el derecho internacional humanitario a las personas más necesitadas,

[24] Véase también Grupo de Asia y el Pacífico sobre Blanqueo de Dinero y Grupo de Acción Financiera de Oriente Medio y África del Norte, “Social media and terrorism financing”, enero de 2019, disponible en www.apgml.org/includes/handlers/get-document.ashx?d=2446bd89-b2cc-4c3c-b378-5f03658dc906.

[25] Grupo de Acción Financiera, *Buenas prácticas: lucha contra el uso indebido de las organizaciones sin ánimo de lucro para la financiación del terrorismo* (París, 2023), párr. 129, disponible en https://biblioteca.gafilat.org/wp-content/uploads/2024/07/Guia-de-Buenas-Practicas-del-GAFI-en-el-Combate-al-uso-indebido-de-las-OSFL-en-FT-R.8.pdf.

sobre todo en zonas afectadas por conflictos o el terrorismo que carecen de servicios bancarios o servicios financieros regulados de otro tipo. Sin los controles adecuados, que incluyan vigilancia y supervisión, la sobrerregulación de los servicios digitales de pago podría imponer cargas onerosas a la labor humanitaria y las actividades legítimas económicas o de las organizaciones sin fines de lucro[26]. El Consejo de Seguridad, en su resolución 2462 (2019), observó con grave preocupación el uso indebido de organizaciones sin fines de lucro por los terroristas para recaudar, trasladar y transferir fondos; exhortó a los Estados Miembros a que aplicaran un enfoque basado en los riesgos y trabajaran en cooperación con el sector sin fines de lucro para prevenir el uso indebido de esas organizaciones, incluido su uso como organizaciones pantalla por los terroristas o en su nombre; y recordó a ese respecto las recomendaciones pertinentes y los documentos de orientación del Grupo de Acción Financiera, en particular su recomendación 8. El Grupo de Acción Financiera también ha observado que el interés de minimizar el impacto negativo en los beneficiarios legítimos de la actividad de las organizaciones sin fines de lucro no puede eludir la necesidad de tomar acciones inmediatas y efectivas para llevar adelante el interés inmediato de detener la financiación del terrorismo u otras formas de apoyo terrorista prestado por las organizaciones sin fines de lucro[27]. El principal objetivo de la recomendación 8 del Grupo de Acción Financiera es velar por que los terroristas no usen de manera indebida las organizaciones sin fines de lucro.

20. A fin de regular, vigilar y supervisar debidamente a los proveedores de servicios de pago nuevos y emergentes, los Estados Miembros deberían considerar lo siguiente:

a) Desarrollar sistemas regulatorios y supervisores basados en riesgos para los sectores pertinentes, entre ellos los proveedores de servicios de activos virtuales, en consonancia con las resoluciones del Consejo de Seguridad y los estándares del Grupo de Acción Financiera sobre la materia, y en plena conformidad con el derecho internacional;

b) Revisar los marcos vigentes con todas las partes interesadas pertinentes de manera constante para que sigan siendo adecuados para afrontar los riesgos nuevos y en evolución, y ampliar esos marcos a los proveedores de servicios nuevos y emergentes, según sea preciso, detectando las carencias y el potencial de duplicación o sobrerregulación;

c) Fortalecer los marcos que permiten la cooperación interinstitucional con miras a intensificar el intercambio oportuno de inteligencia financiera, a nivel nacional e internacional[28], conforme a las recomendaciones del Grupo de Acción Financiera aplicables;

d) Velar por que los marcos nacionales de lucha contra el blanqueo de dinero y la financiación del terrorismo basados en los riesgos se apliquen a los proveedores de servicios de activos virtuales en consonancia con los estándares del Grupo de Acción Financiera a fin de garantizar la rastreabilidad de las transacciones, entre otras cosas mediante la implementación de la denominada “regla de viaje del Grupo de Acción Financiera”, que requiere que los proveedores de servicios de activos virtuales y otras instituciones financieras compartan información relevante sobre el ordenante y el beneficiario en determinadas transacciones de activos virtuales;

[26] En este sentido y respecto de la resolución 2462 (2019), el Grupo de Acción Financiera también reconoce la importancia de garantizar que la aplicación de sus recomendaciones, en particular la 8, cuyo objetivo es velar por que los terroristas y las organizaciones terroristas no utilicen indebidamente las organizaciones sin fines de lucro, no afecte de forma adversa y desproporcionada a las organizaciones sin fines de lucro y, además, no obstaculice indebidamente a la sociedad civil y la prestación de ayuda humanitaria (*ibid.*, párr. 113).

[27] Grupo de Acción Financiera, nota interpretativa de la recomendación 8, párr. 5 d).

[28] Véanse también la resolución 2462 (2019); y S/2021/972, anexo, párr. 673.

e) Desarrollar marcos y mecanismos nacionales adecuados y eficaces para detectar a los proveedores no registrados que operan servicios financieros nuevos y emergentes y realizan transacciones con fondos usando nuevas tecnologías;

f) Aumentar la eficacia de la vigilancia del cumplimiento entre los proveedores registrados de servicios financieros que operan tecnologías nuevas y emergentes (incluidos los operadores de dinero móvil) desarrollando programas eficaces de supervisión del cumplimiento, entre otras cosas mediante la aplicación de procedimientos sólidos de incorporación inicial y diligencia debida con respecto al cliente;

g) Hacer pruebas de las innovaciones del mercado para comprobar que satisfagan las necesidades de los públicos destinatarios al tiempo que respeten los estándares (por ejemplo, las denominadas “zonas de pruebas regulatorias”, donde se puede utilizar un producto de forma condicional con arreglo a una autorización sin objeciones concedida por la instancia reguladora). Cuando se establecen simultáneamente, esos mecanismos podrían facilitar la colaboración del sector privado y las instancias reguladoras con miras a detectar riesgos, afianzar el entendimiento mutuo y probar un marco regulatorio;

h) Desarrollar marcos para vigilar, detectar e interrumpir el uso indebido de las plataformas de medios sociales con fines de financiación del terrorismo, al tiempo que se vela por el pleno cumplimiento del derecho internacional aplicable;

i) Implementar de manera constante iniciativas de divulgación y concienciación dirigidas a los proveedores de servicios pertinentes y otras partes interesadas potencialmente vulnerables que no estén sujetas a la obligación de notificar en relación con la lucha contra el blanqueo de dinero y la financiación del terrorismo, entre ellas los medios sociales y determinadas plataformas de financiación colectiva, para avisarlos de los riesgos de financiación del terrorismo, las tipologías y las señales de alarma, así como de las regulaciones vigentes y los instrumentos disponibles para mitigar o notificar la actividad sospechosa;

j) Adoptar un enfoque multipartito que cuente con la participación significativa de, entre otros, el sector privado, la sociedad civil y el público, al diseñar medidas de mitigación del riesgo de financiación del terrorismo.

Principio rector no vinculante 3: detectar e interrumpir de manera efectiva el uso indebido de las nuevas tecnologías con fines de financiación del terrorismo

21. Los Estados deberían evitar que se politicen las cuestiones de cooperación internacional en la lucha contra el terrorismo, incluida la lucha contra el blanqueo de dinero y la financiación del terrorismo, y seguir mejorando su capacidad de detectar e interrumpir de manera efectiva el uso indebido de las nuevas tecnologías con fines de financiación del terrorismo, entre otras cosas mediante investigaciones y enjuiciamientos penales, una cooperación interinstitucional e internacional reforzada, el establecimiento y la utilización de mecanismos pertinentes para prestar asistencia judicial recíproca y el desarrollo de alianzas público-privadas. Como señaló el Grupo de Acción Financiera[29], las estrategias de interrupción de la financiación del terrorismo abarcan un amplio abanico de instrumentos y prácticas, implementados por numerosas autoridades de lucha contra el terrorismo y la financiación del terrorismo, que trabajan coordinándose entre sí e intercambiando información de manera oportuna. En este sentido, los comités nacionales de coordinación desempeñan una función esencial para formular y aplicar estrategias eficaces de interrupción de la financiación del terrorismo. Una estrategia nacional de lucha contra

[29] Grupo de Acción Financiera, “Terrorist financing disruption strategies”, octubre de 2018 (documento no público).

el terrorismo y la financiación del terrorismo que se base en una evaluación de riesgos exhaustiva y actualizada proporciona el marco para la cooperación operacional entre los organismos competentes y entre estos y el sector privado, entre otras cosas respecto de las tecnologías financieras nuevas y en evolución. Por tanto, las estrategias de interrupción de la financiación del terrorismo van más allá de las investigaciones reactivas y tienen por objeto hacer uso de la gama completa e interdisciplinar de medidas jurídicas, administrativas y de política para interrumpir y minar la capacidad de operar de los grupos terroristas. En la gama de acciones dirigidas a interrumpir la actividad de objetivos concretos se podrían incluir las sanciones financieras específicas; los avisos y las alertas no públicos; la interrupción física del transporte y el almacenamiento de efectivo; las sanciones penales contra terroristas, facilitadores y financiadores; y el decomiso sin condena contra entidades vinculadas a terroristas. Las peculiaridades de cada método de financiación, y los agentes que intervienen, dictarán la respuesta adecuada en cada caso.

22. A fin de detectar e interrumpir de manera efectiva el uso indebido de las nuevas tecnologías con fines de financiación del terrorismo, los Estados Miembros deberían considerar lo siguiente:

a) Desarrollar mecanismos de coordinación multiinstitucionales y, de ser necesario, multipartitos que incluyan a instancias normativas, autoridades de la administración de justicia y las fuerzas del orden, dependencias de investigación financiera, autoridades supervisoras e instancias reguladoras a fin de intercambiar información e inteligencia financiera[30];

b) Establecer marcos y procedimientos para mecanismos de recopilación de observaciones entre las fuerzas del orden, las unidades de inteligencia financiera y las entidades informantes de los sectores pertinentes para mejorar la calidad de los informes y los productos de la inteligencia financiera, así como para contribuir a la vigilancia de tendencias y el análisis estratégico;

c) Desarrollar y aumentar, de manera constante, la capacidad de las autoridades nacionales competentes para seguir la pista del dinero de manera más eficaz, entre otras cosas mediante investigaciones financieras paralelas en casos de terrorismo, utilizando métodos analíticos, instrumentos y tecnologías nuevos, así como los mecanismos independientes de supervisión y examen necesarios. Resulta esencial seguir invirtiendo en tecnologías y capacitación y movilizando a los expertos reputados, así como invertir en tecnología de mejora de la privacidad para proteger la información sensible;

d) Hacer un uso óptimo de las tecnologías financieras y regulatorias nuevas y emergentes para contribuir a la aplicación efectiva de las medidas de lucha contra el blanqueo de dinero y la financiación del terrorismo[31]. La tecnología se debería utilizar de manera responsable para facilitar la reunión, el procesamiento y el análisis de datos y ayudar a detectar y gestionar los riesgos de financiación del terrorismo de manera más eficaz y oportuna;

e) Incluir protecciones y funciones adecuadas para las nuevas soluciones de lucha contra el blanqueo de dinero y la financiación del terrorismo, entre ellas la rendición de cuentas y la transparencia de los procesos y los resultados, la supervisión humana, el respeto de la privacidad y la protección de datos[32] y la armonización con los estándares técnicos y las mejores prácticas a escala mundial;

[30] Véase también la resolución 2462 (2019), párr. 19.

[31] Véase Grupo de Acción Financiera, *Opportunities and Challenges of New Technologies for AML/CFT*.

[32] Véase también la recomendación 2 del Grupo de Acción Financiera, que resalta que el intercambio de información debe incluir cooperación y coordinación entre las autoridades

f) Formular y aplicar políticas y procedimientos destinados a las fuerzas del orden y otras autoridades competentes para investigar el uso de Internet y los medios sociales para la financiación del terrorismo[33] y para obtener acceso a las pruebas de manera oportuna, en pleno cumplimiento del derecho internacional aplicable. Aumentar las capacidades de investigación en medios sociales en relación con la financiación del terrorismo es importante, al igual que lo es desarrollar procedimientos operativos especiales para interactuar con los operadores y los proveedores de servicios en otras jurisdicciones[34];

g) Velar por que los mecanismos establecidos para aplicar los requisitos de congelación de los activos de terroristas sin dilación se apliquen también de manera efectiva a las transacciones de activos mediante tecnologías financieras nuevas y emergentes, entre otros los activos virtuales, respetando plenamente las garantías procesales y los procedimientos reglamentarios;

h) Incluir las direcciones de las billeteras vinculadas directamente a personas o entidades designadas como terroristas en la información identificativa que se comunica al sector privado;

i) Habida cuenta del carácter transfronterizo de la amenaza, compartir con prontitud información de tipo alerta temprana y, de ser necesario, inteligencia financiera entre Estados[35], entre otras cosas respecto de la actividad sospechosa de proveedores de servicios de activos virtuales;

j) Hacer pleno uso de los instrumentos internacionales y regionales de intercambio de información y cooperación, entre otros las bases de datos y los archivos analíticos correspondientes de la Organización Internacional de Policía Criminal, y compartir los conocimientos técnicos y de otro tipo adquiridos para uso de otros Estados Miembros;

k) Potenciar la colaboración con la Dirección Ejecutiva del Comité contra el Terrorismo, el Grupo de Acción Financiera, los organismos regionales al estilo del Grupo de Acción Financiera y otras organizaciones internacionales y regionales competentes para estudiar más maneras de aumentar la eficacia de la respuesta internacional al uso de nuevos métodos de pago y de recaudación de fondos con fines terroristas y establecer una puesta en común periódica de prácticas eficaces en este ámbito;

l) Forjar alianzas público-privadas sólidas para intercambiar información, mejorar la comprensión de las tendencias en evolución, enriquecer los conocimientos y las aptitudes de los expertos y las partes interesadas pertinentes, entre ellos quienes controlan el acceso, y contribuir a fortalecer la integridad del sector financiero[36].

---

competentes para garantizar la compatibilidad de los requisitos de la lucha contra la financiación del terrorismo con las normas de protección de datos y privacidad y otras disposiciones similares (es decir, seguridad y localización de datos).

[33] Véase también Grupo de Asia y el Pacífico sobre Blanqueo de Dinero y Grupo de Acción Financiera de Oriente Medio y África del Norte, “Social media and terrorism financing”.

[34] Véase también Tom Keatinge y Florence Keen, “Social media and terrorist financing: what are the vulnerabilities and how could public and private sectors collaborate better?”, Global Research Network on Terrorism and Technology: Paper No. 10 (Royal United Services Institute for Defence and Security Studies, 2019), disponible en https://static.rusi.org/20190802_grntt_paper_10.pdf.

[35] Véase también la resolución 2462 (2019), párr. 28 a).

[36] Véase también *ibid.*, párr. 22. Durante las sesiones técnicas dirigidas por la Dirección Ejecutiva del Comité contra el Terrorismo, se citó la experiencia del grupo de tareas de financiación del terrorismo del Centro Especializado Financiero en el Reino de los Países Bajos como buena práctica de cooperación e intercambio de información entre el sector público y el privado. Como tendencia general, los Estados que han establecido alianzas público-privadas comunican un aumento de la calidad y la cantidad de los informes de operaciones sospechosas recibidos en

Esas alianzas deberían incluir el diálogo entre las unidades de inteligencia financiera y el sector de tecnologías financieras correspondiente respecto del intercambio de datos como parte de la notificación de actividades sospechosas[37], con una base jurídica clara para el intercambio de información, como criterios y propósitos para los que se pueda intercambiar información y las entidades con las que se pueda hacer el intercambio. Respecto de los medios sociales, estas alianzas público-privadas contribuyen a garantizar que las iniciativas de lucha contra la financiación del terrorismo de las compañías de medios sociales estén informadas y sean eficaces[38]. Las alianzas público-privadas también han servido como foro útil donde las autoridades difunden periódicamente orientaciones sobre tendencias y tipologías destinadas al sector privado, entre otras cosas indicadores de riesgo;

m) Aprovechar las alianzas público-privadas eficaces para utilizar la tecnología y los datos disponibles, entre ellos la inteligencia sobre la cadena de bloques, a fin de reforzar el análisis operacional y táctico, trazar las redes de financiación del terrorismo y rastrear y notificar la actividad sospechosa.

Principio rector no vinculante 4: evaluar las repercusiones de las medidas de lucha contra la financiación del terrorismo en relación con las tecnologías nuevas y emergentes

23. Las instancias reguladoras se enfrentan a la dificultad de equilibrar la necesidad de fomentar nuevas tecnologías de pago por el bien público y al mismo tiempo garantizar un sistema regulador eficaz que proteja ante el uso indebido con fines delictivos y terroristas. Como se ha señalado, la tecnología es capaz de mejorar la rastreabilidad de las transacciones financieras y facilitar la diligencia debida en el ámbito bancario y, por tanto, reducir las cargas y las demoras que repercuten en la labor de las organizaciones sin fines de lucro y los agentes humanitarios. Al mismo tiempo, como subraya el Grupo de Acción Financiera, es necesario "asegur[arse] de que estas soluciones tecnológicas no tengan carácter discriminatorio ni se utilicen de forma discriminatoria"[39].

24. A fin de evaluar las repercusiones y las consecuencias inesperadas que puedan tener las nuevas medidas de lucha contra la financiación del terrorismo en relación con las nuevas tecnologías en los derechos humanos, la inclusión financiera, las actividades legítimas de las organizaciones sin fines de lucro y las actividades de carácter exclusivamente humanitario que lleven a cabo agentes humanitarios imparciales de manera compatible con el derecho internacional humanitario[40] y mitigar de manera eficaz esas consecuencias, los Estados deberían considerar lo siguiente:

a) Instaurar políticas claras, transparentes, sensibles al género y conformes al derecho internacional de los derechos humanos que orienten sobre el uso de las nuevas tecnologías y velen por que se examinen cuidadosamente los riesgos y las consecuencias potenciales;

---

relación con la financiación del terrorismo. Véanse también S/2020/493, párr. 68; y S/2021/972, anexo, párr. 677.

[37] Véase también Stephen Reimer y Matthew Redhead, *Bit by Bit: Impacts of New Technologies on Terrorism Financing Risks*, RUSI Occasional Paper (Royal United Services Institute for Defence and Security Studies, 2022).

[38] Véase también Keatinge y Keen, "Social media and terrorist financing".

[39] Grupo de Acción Financiera, *Buenas prácticas: lucha contra el uso indebido de las organizaciones sin ánimo de lucro para la financiación del terrorismo*, párr. 129. El Grupo de Acción Financiera señala en particular que "puede ser necesaria la supervisión humana cuando se utilicen algoritmos para evitar perpetuar los prejuicios existentes (religiosos, étnicos, de género y otros)".

[40] Véase también la resolución 2462 (2019), quinto párrafo del preámbulo y párrs. 23 y 24.

b) Adoptar un enfoque multipartito al examinar y gestionar de manera proactiva cualquier repercusión adversa, potencial o real, de las medidas de lucha contra la financiación del terrorismo en relación con las nuevas tecnologías en los derechos humanos, desarrollar directrices, instrumentos de examen y parámetros de referencia para esas evaluaciones de las repercusiones y elaborar medidas de mitigación, incluyendo a las autoridades nacionales competentes, el sector privado, la sociedad civil y el mundo académico. Además, la existencia de mecanismos, plataformas o canales específicos permanentes puede ayudar a que la sociedad civil y otras partes interesadas pertinentes comuniquen de manera eficaz cualquier consecuencia adversa inesperada que las medidas de lucha contra la financiación del terrorismo recién desarrolladas tengan para el ejercicio de sus derechos y sus actividades legítimas y, de ser necesario, solicitar una revisión judicial;

c) Al diseñar sistemas de datos y procesos que faciliten el acceso, la recuperación y el análisis de información pertinente (entre otras cosas usando el aprendizaje automático y automatizando la detección de riesgos de delitos financieros), velar por que existan marcos y protocolos de intercambio de datos a fin de facilitar el intercambio de información entre las diferentes entidades que participen en la lucha contra la financiación del terrorismo, de conformidad con el derecho internacional de los derechos humanos;

d) Al evaluar la eficacia, adoptar un enfoque basado en datos e inclusivo para lograr información útil. Revisando y analizando de forma periódica los datos relevantes, las instancias normativas y las partes interesadas pueden descubrir aspectos que necesitan mejorar, perfeccionar estrategias y aumentar la eficacia general de las iniciativas de lucha contra la financiación del terrorismo;

e) A medida que las tecnologías financieras siguen cambiando y su uso en la lucha contra el blanqueo de dinero y la financiación del terrorismo va aumentando, reforzar los mecanismos independientes de supervisión y rendición de cuentas para las medidas correspondientes de conformidad con las garantías procesales y los procedimientos reglamentarios. Los mecanismos de supervisión deberían también velar por que las alianzas público-privadas pertinentes cumplan las obligaciones en materia de protección de datos o privacidad que les incumben en virtud de la legislación nacional y el derecho internacional aplicable;

f) Velar por que las medidas creadas para hacer frente a los riesgos de financiación del terrorismo detectados en relación con las nuevas tecnologías de pago no obstaculicen indebidamente ni afecten de forma negativa las actividades legítimas de las organizaciones sin fines de lucro. Los Estados deberían considerar si las medidas específicas, proporcionales y basadas en los riesgos ya aplicadas en relación con el subgrupo de organizaciones sin fines de lucro definido por el Grupo de Acción Financiera[41], incluidas las medidas de autorregulación y las medidas internas de

[41] A efectos de la recomendación 8 del Grupo de Acción Financiera, “organización sin fines de lucro” se refiere a una persona o estructura jurídica u organización que principalmente se dedica a la recaudación o desembolso de fondos para fines tales como propósitos caritativos, religiosos, culturales, educativos, sociales o fraternales, o para la realización de otros tipos de “buenas obras”. En 2016 se revisó esta recomendación para definir claramente el subgrupo de organizaciones sin fines de lucro que debían estar sometidas a supervisión y vigilancia. Tras la revisión de noviembre de 2023, la recomendación 8 y su nota interpretativa piden “medidas focalizadas, proporcionales y basadas en riesgo, sin perjudicar o desalentar indebidamente las actividades legítimas de las [organizaciones sin fines de lucro]”, a fin de proteger a ese sector frente a la financiación del terrorismo. Según la nota interpretativa de la recomendación 8 del Grupo de Acción Financiera (párr. 6):

“Las [organizaciones sin fines de lucro] corren diversos grados de riesgo de abuso de [financiación del terrorismo] en virtud de sus tipos, actividades o características y la mayoría puede representar bajo riesgo. Sin perjuicio de los requisitos de la recomendación 1:

mitigación de riesgos, pueden servir también para hacer frente a los nuevos riesgos y vulnerabilidades;

g) Establecer mecanismos, plataformas o canales permanentes para que la sociedad civil y otras partes interesadas pertinentes puedan comunicar cualquier consecuencia adversa inesperada que las medidas de lucha contra la financiación del terrorismo recién desarrolladas tengan para el ejercicio de sus derechos y sus actividades legítimas y, de ser necesario, solicitar una revisión judicial. La labor de divulgación debería incluir un diálogo fructífero y colaborativo entre la administración, el sector privado y la sociedad civil, entre otras cosas sobre las dificultades y las consecuencias imprevistas;

h) Velar por que las nuevas regulaciones creadas para mejorar la rastreabilidad y la transparencia de las transacciones financieras no vulneren el derecho a no sufrir injerencias ilícitas o arbitrarias en el derecho a la privacidad y otros derechos humanos, ni tengan como resultado la vigilancia de los beneficiarios de la ayuda humanitaria, sino que refuercen las protecciones de la privacidad mediante el uso lícito de la información personal;

i) Proporcionar al sector privado orientación sobre la eliminación del sesgo y los datos erróneos en los modelos de detección, entre otras cosas mediante mecanismos para que las personas aporten sus observaciones, y la manera más eficaz de intercambiar datos con las autoridades de conformidad con el derecho internacional de los derechos humanos aplicable;

j) Investigar más y crear unos estándares mínimos para la eficacia de la tecnología financiera y sus repercusiones en los diferentes grupos de partes interesadas;

k) Documentar las buenas prácticas y las enseñanzas extraídas sensibles al género y conformes al derecho internacional de los derechos humanos sobre el diseño, el desarrollo y la evaluación de tecnologías de lucha contra el blanqueo de dinero y la financiación del terrorismo, con participación del sector privado y la sociedad civil.

a) Los países deben identificar organizaciones que caen dentro de la definición de [organización sin fines de lucro] del GAFI.

b) Los países deben realizar una evaluación de riesgos de estas [organizaciones sin fines de lucro] para identificar la naturaleza de los riesgos de [financiación del terrorismo] que se les presentan”.