Detección y desarticulación de las actividades del financiamiento al terrorismo

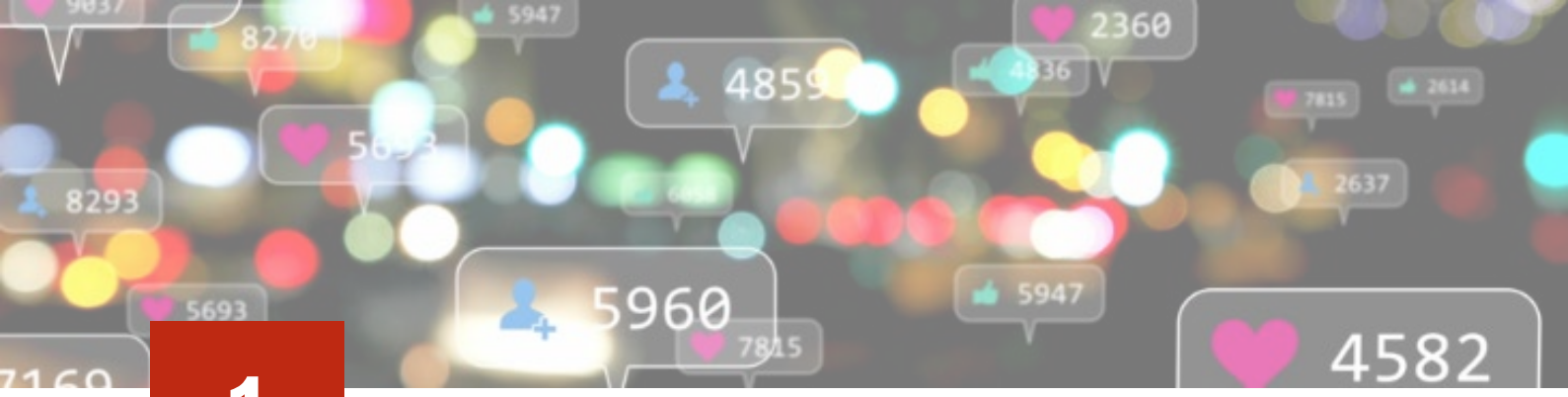
A TRAVÉS DE LAS REDES SOCIALES, APLICACIONES DE MENSAJERÍA INSTANTÁNEA Y PLATAFORMAS DE STREAMING

Junio de 2026

TRADUCCIÓN NO OFICIAL

Esta es una traducción no oficial elaborada por la delegación de México con fines meramente informativos. El GAFI no puede garantizar la exactitud de esta traducción. La única versión oficial es el texto en inglés disponible en la página web del GAFI *https://www.fatf-gafi.org/en* en la siguiente URL: https://www.fatf-gafi.org/en/publications/Methodsandtrends/detecting-and-disrupting-tf-through-smsps.html

En caso de discrepancia entre la versión oficial y esta traducción, solo se considerará válido el texto de la versión oficial en inglés.



1

Introducción

01. La lucha contra el financiamiento al terrorismo (CFT) sigue siendo una prioridad para el Grupo de Acción Financiera (GAFI), dadas las graves amenazas persistentes y en constante evolución, que plantean las organizaciones e individuos terroristas en todo el mundo. Estas amenazas abarcan desde pequeñas células hasta grandes organizaciones en red que operan a través de las fronteras y/o poseen capacidad para ejercer control territorial.

02. Los terroristas han demostrado su capacidad persistente para hacer uso indebido del sistema financiero internacional con el fin de recaudar, mover, almacenar y gastar fondos para satisfacer sus necesidades financieras y operativas. Los métodos de financiamiento utilizados por los actores terroristas pueden variar considerablemente, en parte en función de su acceso a las tecnologías emergentes, plataformas digitales, redes sociales, aplicaciones de mensajería instantánea y plataformas de streaming (SMSP, por sus siglas en inglés), así como de su capacidad para adaptar sus métodos de financiamiento a las nuevas tecnologías disponibles.

Partiendo de la «Actualización Exhaustiva sobre los Riesgos de Financiamiento al Terrorismo» (2025) del GAFI, los miembros del GAFI decidieron profundizar en su conocimiento sobre cómo las SMSP pueden ser objeto de abuso con fines de financiamiento al terrorismo. El presente documento sensibiliza al público y a las partes interesadas sobre las cuestiones identificadas por el GAFI con el fin de apoyar a las autoridades operativas en la detección, desarticulación, investigación y enjuiciamiento de las actividades de financiamiento al terrorismo que puedan tener lugar en las SMSP.

El ecosistema de las SMSP y su exposición al riesgo de FT

El ecosistema de las SMSP abarca desde las redes sociales convencionales hasta las aplicaciones de mensajería cifrada, y está diseñado para garantizar la accesibilidad y la escalabilidad. Las funcionalidades principales de estas redes y aplicaciones incluyen la mensajería instantánea, el intercambio de contenidos multimedia, la creación de grupos y, **cada vez más, la disponibilidad de funciones de pago integradas en la interfaz de usuario o habilitadas a través de socios comerciales externos.**

Las SMSP han **pasado de ser meras herramientas de comunicación a convertirse en ecosistemas digitales más complejos** que integran servicios financieros y fuentes de ingresos. Por lo general, las SMSP y los grandes proveedores de tecnología o telecomunicaciones no prestan servicios de pago directamente, sino que operan como plataformas a través de las cuales, terceros proveedores de servicios de pago (PSP), regulados o no, se integran y ofrecen dichos servicios. Las obligaciones en materia de lucha contra el lavado de dinero y el financiamiento al terrorismo (PLD/CFT) se aplican a estos PSP en función de la materialidad y la naturaleza de sus actividades. Los continuos avances tecnológicos requieren un seguimiento constante, ya que las sucesivas generaciones de sistemas de pago se integran cada vez más profundamente en las interfaces de las plataformas, lo que puede difuminar los límites regulatorios tradicionales.

La exposición al riesgo de las SMSP se refiere principalmente a su posible uso para la recaudación y el movimiento de fondos, lo que difiere de su función en la comunicación y el intercambio de contenidos. A medida que se expande el ecosistema de las SMSP, se prevé que este riesgo aumente.

Las jurisdicciones que han contribuido a este trabajo destacaron una distribución casi equitativa de las amenazas terroristas que abusan de las SMSP con fines de financiamiento: se señaló que abusaban de este ecosistema los terroristas individuales, incluidos los combatientes terroristas extranjeros y las pequeñas células (30%), las organizaciones e individuos terroristas con motivaciones étnicas o raciales (26%), las grandes organizaciones en red que dependen de filiales regionales y nacionales (25%) y los grupos terroristas regionales y nacionales no afiliados (19%).

Además, menos del 30% de las jurisdicciones que contribuyeron a este informe incluyen los riesgos de financiamiento al terrorismo a través de las SMSP en sus evaluaciones nacionales de riesgos, y el 38% de ellas calificaron dicho riesgo en sus países como moderado. Al mismo tiempo, en zonas de conflicto y/o áreas que se enfrentan a amenazas terroristas activas, el riesgo de que las SMSP sean utilizadas indebidamente con fines de FT se califica generalmente como alto o muy alto.

Las SMSP influyen en el panorama de riesgo de la FT debido a sus características fundamentales: (i) su acceso y alcance transnacionales; (ii) su amplia base de usuarios gracias a su creciente adopción; (iii) la rapidez en la recopilación y el intercambio de información; y (iv) el uso de sistemas de filtrado, incluidos algoritmos para recomendar y promover contenidos basados en los usuarios. Junto con las tecnologías que refuerzan el anonimato, estas características permiten a las organizaciones criminales y a los grupos terroristas operar a escala transnacional y aumentar la efectividad de sus actividades ilícitas.

Diferencias en el uso de las SMSP con fines de terrorismo y de FT

Distinguir entre el uso de las SMSP para actividades relacionadas con el terrorismo y para fines de FT sigue siendo un reto para las autoridades competentes, sobre todo dada la superposición entre las actividades de comunicación, propaganda, reclutamiento y actividades financieras que tienen lugar a través de estas plataformas. Además, la mayoría de los mecanismos de aplicación y cumplimiento implementados por las SMSP se centran principalmente en la detección y eliminación de contenidos terroristas y extremistas, mientras que los mecanismos de aplicación destinados a identificar y desarticular las actividades de FT aún se encuentran en fase de desarrollo.

Los grupos terroristas suelen aprovechar el alcance y la dinámica viral de las redes sociales, y las aplicaciones de mensajería cifrada pueden facilitar aún más la coordinación operativa al permitir la comunicación, el intercambio de información, la obtención de influencia, la recaudación de fondos en línea y la logística de las donaciones, en lugar de las transacciones financieras directas.

El uso de las SMSP con fines de FT implica el aprovechamiento de las funcionalidades financieras de las plataformas y de los mecanismos informales de transferencia de transferencia de valor. Las aplicaciones de mensajería con sistemas de pago integrados, como los monederos de activos virtuales (AV) o funciones similares, permiten realizar transferencias entre particulares (P2P) para eludir los requisitos aplicables en materia de debida diligencia del cliente (DDC).

La tabla siguiente describe brevemente las principales diferencias en la naturaleza del uso indebido de las SMSP:

	Uso indebido con fines de terrorismo	Uso indebido con fines de FT
Objetivo principal	Difundir propaganda, reclutar miembros y coordinar operaciones (actos terroristas)	Recaudar, transferir y ocultar fondos para financiar las actividades de las organizaciones terroristas
Actividades principales	Difusión de contenidos relacionados con actividades terroristas, planificación operativa cifrada, creación de redes	Financiamiento colectivo, transferencias P2P, uso de sistemas de pago integrados
Características clave aprovechadas	Compartir contenido viral, anonimato, cifrado	Débiles medidas de DDC, opciones de pago transfronterizo, integración de activos virtuales (AV)
Naturaleza del abuso	Ideológico y logístico	Financiero y transaccional
Dificultades de detección	Supervisión de las comunicaciones cifradas y moderación de contenidos	Seguimiento de transacciones pequeñas y frecuentes y de transferencias informales de valor

2 Tendencias y tipologías clave

Repercusiones en el panorama de riesgos de FT y respuesta necesaria

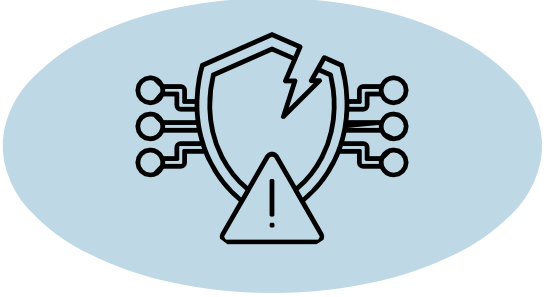
- **Difuminación de las responsabilidades regulatorias**: A medida que las SMSP integran funcionalidades financieras a través de sus interfaces o de socios externos, se necesitan marcos más claros para determinar qué servicios están sujetos a las obligaciones en materia de PLD/CFT y qué entidad debe cumplirlas.
- **Mayor complejidad operativa y opacidad**: Las tecnologías avanzadas permiten actividades de FT más rápidas, más estratificadas y más difíciles de detectar, lo que exige una adaptación continua de las evaluaciones de riesgo y las tipologías.
- **Vulnerabilidades emergentes en los modelos de monetización**: Las nuevas fuentes de ingresos (por ejemplo, las retransmisiones en directo, suscripciones, propinas digitales) crean nuevas vías de FT que requieren una supervisión específica.
- **La rápida evolución tecnológica está redefiniendo los riesgos del financiamiento al terrorismo**: nuevas características como los contenidos generados por IA, las comunicaciones cifradas, los AV, las finanzas descentralizadas (DeFi) y las herramientas de pago integradas amplían continuamente las formas en que se puede hacer uso indebido de las SMSP, y las autoridades competentes deben mantenerse al día en la comprensión de los riesgos potenciales en caso de abuso.

Las tipologías identificadas de SMSP con fines de FT son las siguientes:

Tipología	Descripción
Fachada humanitaria y organizaciones benéficas falsas	Uso de las redes sociales para recaudar fondos mediante llamamientos humanitarios o benéficos fraudulentos, a menudo dirigidos a las diásporas y basados en microdonaciones, que se aprovechan de la confianza de los usuarios y del alcance de las plataformas para ocultar la verdadera intención y reducir el escrutinio. Las organizaciones o páginas de fachada recaudan fondos que se desvían hacia fines terroristas, a veces junto con contenido relacionado con el terrorismo.
Uso multiplataforma y multimodal de las SMSP	La recaudación de fondos comienza en las principales plataformas de redes sociales y se traslada a servicios de mensajería cifrada o grupos privados para la coordinación y las instrucciones de pago, lo que reduce la visibilidad y permite un intercambio seguro de datos financieros. Los datos de pago (cuentas, monederos electrónicos, instrucciones codificadas) se intercambian directamente entre miembros de confianza.
Métodos de pago fuera de la plataforma y diversificados	Redirección a canales de pago externos (transferencias bancarias, proveedores de sistemas de pago de terceros, activos virtuales, recaudación de efectivo, tarjetas de prepago), a menudo combinados con sistemas de transferencia informales (p. ej. hawala) para ocultar el rastro de las transacciones. Las donaciones en línea se convierten en efectivo o en valor a través de hawala, dinero móvil, recogidas de efectivo, tarjetas prepago, créditos de tiempo aire o vales digitales para ocultar el rastro de las transacciones.
Aprovechamiento de las funciones y herramientas de amplificación de las plataformas	Uso de anuncios de pago o contenido promocionado, bots, cuentas falsas o comprometidas, y funciones de la economía de los creadores (p. ej. retransmisiones en directo, propinas) para aumentar el alcance, la legitimidad y la generación de ingresos.
Recaudación de fondos a través de AV y carteras integradas en la aplicación	Uso de carteras de AV (incluidas las carteras integradas en la plataforma) y códigos QR para transferencias transfronterizas, a menudo con direcciones rotativas y una DDC limitada, lo que aumenta el anonimato y reduce la trazabilidad.
Camuflaje, comunicación codificada y técnicas de evasión	Los actores terroristas emplean lenguaje codificado, emojis, números y referencias internas para señalar actividades de recaudación de fondos al tiempo que evitan ser detectados, a menudo disfrazando las solicitudes como apoyo humanitario, religioso o comunitario. Uso de lenguaje codificado, símbolos, eslóganes y narrativas humanitarias o religiosas para ocultar la intención, evadir la detección y reforzar la identidad de grupo, a menudo combinado con comunicaciones cifradas o efímeras.
Actividad comercial encubierta (estratificación)	La recaudación de fondos se disfraza de ventas en línea, publicaciones de mercados en línea o eventos con entrada, lo que permite mezclar los ingresos con transacciones de apariencia legítima.
Adquisición de bienes en especie	Los fondos recaudados en línea se utilizan directamente para adquirir bienes (p. ej. alimentos, combustible, equipamiento o suministros) que se entregan a nivel local, eludiendo los canales financieros formales.

Tipología	Descripción
Productos de la extorsión y el secuestro	Las aplicaciones de mensajería se utilizan para comunicar las exigencias, coordinar los pagos y transferir los ingresos procedentes de la extorsión o el secuestro a través de canales digitales o informales.
Dirigidas a jóvenes y colectivos vulnerables	Los actores terroristas se dirigen deliberadamente a personas jóvenes y socialmente vulnerables mediante llamados de carácter emocional y con un enfoque humanitario en plataformas populares entre estos grupos, aprovechando la empatía, la identidad y el sentido de pertenencia para generar donaciones y, en algunos casos, una radicalización más amplia.
Fomento de la confianza y participación digital personalizada para la movilización	Las redes utilizan mensajes continuos, la validación entre iguales y contenidos personalizados (incluidos idiomas locales, narrativas orientadas a los jóvenes y la amplificación mediante inteligencia artificial (IA) en todas las plataformas) para ganar credibilidad con el tiempo, integrando las solicitudes de donaciones en comunidades de confianza y convirtiendo progresivamente a los usuarios en colaboradores económicos o facilitadores.
Aprovechamiento de las características de la economía de los creadores para la recaudación de fondos	Los actores terroristas y sus simpatizantes generan ingresos a través de herramientas de monetización de las plataformas —como las retransmisiones en directo, las donaciones colectivas y los ingresos basados en la interacción—, lo que difumina la línea entre los ingresos legítimos y los fondos vinculados a los ecosistemas extremistas. La monetización basada en contenidos se caracteriza por ser una vía de FT, ya que los contenidos se aprovechan como un activo generador de ingresos, y los mecanismos de pago agregados ocultan las fuentes de financiamiento y permiten a las personas acumular y, potencialmente, redirigir los ingresos hacia actividades relacionadas con el terrorismo.
Uso indebido de los sistemas de pago integrados en la interfaz de las SMSP	Los actores terroristas explotan las funciones de monedero integradas para enviar, recibir e intercambiar AV directamente dentro de las plataformas de mensajería, lo que permite una recaudación de fondos y transferencias fluidas con una menor dependencia de los sistemas financieros externos. La combinación de monederos integrados en la aplicación y canales de comunicación cifrados permite a los actores maliciosos llevar a cabo campañas de recaudación de fondos —especialmente vinculadas a zonas de conflicto— al tiempo que ocultan sus identidades, aumentan la adopción y dificultan los esfuerzos de detección y desarticulación.
Uso de factores contextuales como catalizadores de campañas de recaudación de fondos en redes sociales	Los actores terroristas aprovechan los conflictos, las crisis humanitarias y los acontecimientos políticos para iniciar y amplificar campañas de recaudación de fondos, presentando sus llamados como esfuerzos humanitarios urgentes o de solidaridad para atraer un amplio apoyo. Al alinear los mensajes con acontecimientos que despiertan emociones y difundirlos rápidamente, estos actores aumentan su legitimidad, amplían su alcance y aceleran las donaciones antes de que se puedan aplicar medidas de detección o contramedidas.

- Las SMSP se utilizan cada vez más como infraestructuras confiables para FT, combinando plataformas públicas para amplificar los mensajes de recaudación de fondos con aplicaciones de mensajería cifrada para la coordinación, el reparto de pagos y el traslado de las actividades a canales privados —a menudo recurriendo a pequeñas donaciones colectivas presentadas como ayuda humanitaria—.
- A medida que las plataformas amplían sus funciones de pago y monetización, los actores terroristas explotan cada vez más estas herramientas para recaudar, mover y gestionar fondos, aprovechando las funcionalidades integradas y los entornos cifrados para coordinar operaciones y evadir la detección.
- Estas tipologías demuestran un alto grado de adaptabilidad, ya que los actores ajustan rápidamente sus métodos en respuesta a las características de las plataformas, las medidas reguladoras y los acontecimientos geopolíticos. En consecuencia, las tipologías observadas en la actualidad seguirán evolucionando, lo que exigirá respuestas basadas en el riesgo y en constante evolución, en lugar de respuestas puntuales.



Situación actual según los Estándares del GAFI

3

Actualmente, las SMSP no se incluyen entre los sectores que deben cumplir con las obligaciones en materia de PLD/CFT según los Estándares del GAFI y, por lo tanto, no se encuentran en la mayoría de los marcos nacionales. **Sin embargo, su evolución progresiva hacia ecosistemas basados en plataformas que integran o facilitan el acceso a una amplia gama de servicios financieros implica que determinadas actividades realizadas a través de las SMSP o facilitadas por éstas pueden entrar en el ámbito de aplicación de sectores ya regulados por los Estándares del GAFI. Las funcionalidades que facilitan la intermediación financiera —como los monederos de activos virtuales y las transacciones con ellos, las transferencias entre particulares (P2P), los mecanismos de pago integrados en aplicaciones,** los mercados, las herramientas de monetización para creadores y el comercio electrónico integrado— pueden dar lugar a la aplicación de las Recomendaciones pertinentes del GAFI, en función de la naturaleza, la escala y el control ejercido por las SMSP o por los proveedores terceros asociados.

A tal efecto, es importante distinguir entre las situaciones en las que el proveedor de SMSP opera como una plataforma neutral que permite a terceros ofrecer servicios financieros, y aquellas en las que el propio proveedor desempeña funciones que entran dentro de la definición de institución financiera (IF) o proveedor de servicios de activos virtuales (PSAV). Cuando una SMSP se limita a proporcionar la infraestructura técnica o la interfaz de usuario a través de la cual proveedores externos autorizados o regulados de otro modo prestan servicios de pago o de activos virtuales, las responsabilidades en materia PLD/CFT pueden recaer principalmente en dichos terceros. En función del grado de control, influencia o beneficio que conserve la SMSP, ésta puede tener algunas obligaciones secundarias u otras. Por el contrario, cuando la SMSP ofrece, controla o influye de manera significativa en los servicios financieros a través de su interfaz (como la custodia, la transferencia, el intercambio o la facilitación de fondos o AV), puede entrar ella misma en la definición de una IF o un PSAV regulado, y las obligaciones correspondientes en materia PLD/CFT pueden aplicarse directamente a la SMSP desde un punto de vista funcional.

Función principal	Finalidad
Compra dentro de la aplicación	Permite a los usuarios comprar bienes virtuales, funciones premium o contenidos directamente dentro de la plataforma. Actúa como punto de entrada para la monetización y las microtransacciones. Es habitual en los videojuegos, las plataformas de creadores y las aplicaciones sociales (por ejemplo, la compra de pegatinas, regalos virtuales o experiencias sin publicidad).
P2P	Permite a los usuarios enviar dinero directamente a otros usuarios dentro de la aplicación. Esto puede referirse a transferencias entre monederos no alojados o simplemente a un pago entre particulares con la intermediación de uno o más proveedores de servicios de pago (PSP).
Pagos a comerciantes	Admite transacciones entre empresas y consumidores a través de pasarelas de pago integradas. Se utiliza para el comercio social (por ejemplo, la compra de productos a influencers o marcas dentro de la aplicación).
Pagos a usuarios/creadores	Las plataformas pagan a los creadores o influencers por contenidos monetizados, anuncios o regalos virtuales. Estos mecanismos financieros son fundamentales para sostener las economías de los creadores e incentivar la participación, y pueden implicar transferencias bancarias directas o pagos a través de carteras.
Integración con monederos de activos virtuales (AV) de terceros	Ofrece una cuenta de valor almacenado dentro de la plataforma para guardar fondos. Permite realizar pagos rápidos por servicios, dar propinas a los creadores o comprar productos. A menudo está vinculada a programas de lealtad o a monederos virtuales.
Integración con servicios bancarios	Va más allá de los pagos para ofrecer funciones similares a las de la banca (por ejemplo, préstamos, ahorros, crédito). Posiciona a las plataformas como actores del sector fintech, reduciendo la dependencia de los bancos tradicionales.
Pagos con AV	Permite realizar transacciones utilizando AV o activos tokenizados. Añade la capacidad de realizar pagos transfronterizos y resulta atractivo para los usuarios con conocimientos tecnológicos.
Integración de carteras de activos virtuales	Las plataformas de activos virtuales se integran en la interfaz de la aplicación de mensajería instantánea, ofreciendo una experiencia de doble monedero: un monedero de activos virtuales con custodia para el público general y un monedero con autocustodia.

Nota: La información proporcionada en la tabla anterior se basa en los datos facilitados por las jurisdicciones al proyecto y en investigaciones de fuentes abiertas. Los modelos de negocio cambian continuamente y esta tabla se ofrece únicamente con fines ilustrativos, sin pretender ser exhaustiva ni constituir una referencia autorizada sobre las actividades que realizan las empresas.

La tabla anterior ayuda a comprender cómo se prestan los servicios financieros —ya sea integrados en la plataforma o mediante redireccionamiento— e identifica los sistemas de pago dentro del ecosistema SMSP que pueden entrar en la definición de IF o PSAV desde una perspectiva funcional.

Las SMSP facilitan los flujos financieros a través de diversos modelos de negocio y mecanismos de monetización que combinan los servicios de comunicación con funcionalidades de pago y otras formas de actividad económica. Es importante que las autoridades competentes comprendan estos modelos, ya que pueden indicar cómo se generan, transfieren o integran los fondos dentro del ecosistema de la plataforma.

Modelo de negocio de las SMSP	Características de monetización
Ingresos procedentes de la publicidad	Las plataformas monetizan la atención de los usuarios mediante la publicación de anuncios altamente segmentados basados en el comportamiento y la interacción. Los ingresos aumentan con la actividad de los usuarios, mientras que los creadores pueden recibir pagos vinculados a métricas de rendimiento (visualizaciones, anuncios, suscriptores).
Personalización y análisis basados en datos	Los datos de los usuarios se aprovechan para mejorar los servicios y optimizar la efectividad de la publicidad. Las plataformas monetizan esta información ofreciendo herramientas de análisis y datos de audiencia a creadores, anunciantes y empresas.
Servicios de suscripción o cuota mensual	Los usuarios pagan cuotas periódicas por funciones premium, como experiencias sin anuncios o herramientas avanzadas. Estas suscripciones suelen incluir contenido exclusivo, funcionalidades mejoradas o mejoras para empresas.
Compras dentro de la aplicación	Los ingresos se generan mediante la venta de productos digitales y mejoras de funciones dentro de la plataforma. Los usuarios pueden mejorar su experiencia comprando artículos virtuales, complementos o funcionalidades premium.
Integración de comercio electrónico o comercio social	Las compras están integradas directamente en la plataforma, lo que permite navegar y comprar sin interrupciones. Las SMSP obtienen ingresos a través de comisiones por transacción, comisiones y colaboraciones, a menudo mediante ventas impulsadas por creadores o compras en directo.
Monetización de la economía de los creadores o marketing de afiliados	Las plataformas permiten a los creadores obtener ingresos a través de suscripciones, propinas, anuncios, productos digitales y regalos virtuales. Algunas utilizan tokens propios que se pueden adquirir con dinero fiduciario y que los creadores pueden convertir posteriormente en efectivo.
Interfaz de programación de aplicaciones (API) y servicios para empresas	Las plataformas ofrecen herramientas de pago para empresas, que incluyen automatización, mensajería, análisis e integración. Los ingresos provienen de cobrar por el uso de gran volumen, las funciones avanzadas y los servicios de nivel empresarial.
Sistemas de plataformas integradas y monetización multiplataforma	Las empresas vinculan múltiples aplicaciones y servicios para maximizar la participación de los usuarios y las oportunidades de venta cruzada. Los ingresos se diversifican a través de anuncios agrupados, suscripciones y herramientas en ecosistemas interconectados.
Funciones de propina	Los usuarios pueden enviar pagos voluntarios a los creadores a través de servicios de pago de terceros vinculados. La plataforma facilita la visibilidad y el acceso, pero no procesa los pagos por sí misma, sino que recurre a proveedores externos.

Nota: La información proporcionada en la tabla anterior se basa en las aportaciones de las jurisdicciones al proyecto, en consultas específicas al sector privado y al ámbito académico, y en investigaciones de código abierto. Los modelos de negocio cambian continuamente y esta tabla se ofrece únicamente con fines ilustrativos, sin pretender ser exhaustiva ni constituir una referencia autorizada sobre las actividades realizadas por las empresas.

Cuando estas actividades las lleve a cabo una SMSP, es importante que las autoridades competentes evalúen si ésta podría, en la práctica, estar actuando como una IF o un PSAV conforme a los Estándares del GAFI. Cuando se identifiquen tales funciones, se aplicarán las obligaciones correspondientes en materia de PLD/CFT. Tal y como se señala en la Recomendación 31, las autoridades competentes deben poder acceder a todos los documentos y la información necesarios para su uso en dichas investigaciones, así como en los procesos judiciales y las acciones relacionadas. Esto debe incluir facultades para aplicar medidas coercitivas con el fin de obtener registros en poder de IF, APNFD y otras personas físicas o jurídicas, para realizar registros de personas y locales, para tomar declaraciones de testigos y para la incautación y obtención de pruebas. Esto resulta especialmente relevante cuando las SMSP conservan o tratan datos vinculados a actividades financieras que suelen llevar a cabo los sectores regulados, ya que puede abrir una serie de oportunidades para rastrear los flujos financieros que se producen en el marco de las funcionalidades de estas plataformas y puede contribuir a comprender los nodos de conexión de las operaciones de financiamiento de las organizaciones terroristas. Cuando se combina con contenidos de dominio público publicados en la plataforma, dicha información puede proporcionar elementos probatorios clave para vincular una cuenta o un usuario con una organización terrorista o una actividad financiera relacionada.

Las SMSP están cada vez más expuestas a flujos financieros debido a la integración de mecanismos de pago en sus plataformas o a través de contenidos generados por los usuarios que incluyen enlaces de pago y transferencia.

4 Necesidades de respuesta operativa y sector privado

Necesidades de respuesta operativa

Ninguna jurisdicción ni autoridad puede abordar los riesgos del FT través de las SMSP de forma aislada. La supervisión, la gestión y la mitigación de estos riesgos requieren una respuesta coordinada y en múltiples niveles por parte de las autoridades nacionales, las asociaciones público-privadas (PPP, por sus siglas en inglés) y la cooperación internacional, con el respaldo de marcos capaces de adaptarse a las tecnologías y a los actores que plantean amenazas, en constante evolución.

La detección eficaz de la actividad de FT a través de las SMSP depende de:

1. **Indicadores de riesgo y factores desencadenantes claros** que ayuden a las autoridades operativas a identificar la actividad delictiva subyacente.
2. **Un enfoque coordinado y en múltiples niveles para identificar, investigar y enjuiciar** el FT a través de las SMSP (por ejemplo, UIF, autoridades de investigación y procuración de justicia y órganos supervisores).
3. **Enfoques de investigación sólidos**, que incluyan inteligencia de fuentes abiertas (OSINT), análisis de redes y técnicas avanzadas de seguimiento.
4. **La colaboración entre las UIF y las entidades reguladas** (por ejemplo, IF, PSAV y APNFD) para acceder a la inteligencia financiera y garantizar la aplicación de la DDC y el monitoreo de las transacciones cuando proceda.
5. Establecimiento de **canales de comunicación bilaterales con las SMSP** para agilizar el intercambio de información sobre casos específicos y tendencias emergentes, incluso a través de asociaciones público-privadas.
6. **Mecanismos de intercambio oportuno de información y de conservación de datos**.

Estas medidas deben ajustarse a los marcos jurídicos aplicables, respetando el derecho internacional humanitario, así como la protección de datos y la privacidad.

Papel del sector privado

El sector privado desempeña un papel fundamental al proporcionar datos, capacidades tecnológicas y mecanismos de detección temprana para identificar y ayudar a desarticular las actividades de FT a través de las SMSP. El sector privado cuenta con la capacidad y los recursos para desarrollar herramientas avanzadas de detección y prevención, incluidas soluciones basadas en la inteligencia artificial para identificar actividades relacionadas con FT en fases tempranas, actuando como primera línea de defensa. Como tal, tiene la capacidad de suspender las transacciones y comunicaciones de los usuarios ante una sospecha razonable de contenido relacionado con el terrorismo y el FT. Estos actores albergan y pueden proporcionar datos críticos, visibilidad y capacidades de las autoridades encargadas de hacer cumplir la ley que complementan y refuerzan la capacidad de las autoridades para detectar y desarticular las actividades de FT. Las SMSP pueden proporcionar señales de detección temprana e información operativa que permitan una actuación más rápida por parte de las autoridades competentes. Esto puede facilitarse si las autoridades proporcionan a las SMSP una descripción clara de los factores contextuales del caso, el delito objeto de investigación, los identificadores relevantes de la actividad y/o los sospechosos investigados.

Un enfoque beneficioso para todas las partes mediante asociaciones público-privadas (PPP, por sus siglas en inglés):

El refuerzo de la cooperación entre el sector tecnológico, las SMSP, IF, los PSP, los PSAV y las autoridades competentes genera beneficios mutuos. A medida que el sector adquiere un conocimiento más profundo de las tendencias del FT, puede diseñar algoritmos y medidas de protección más efectivas para prevenir el uso indebido, al tiempo que protege y potencia la actividad empresarial legítima. Al mismo tiempo, las autoridades de investigación y procuración de justicia (LEA, por sus siglas en inglés) se benefician de un acceso más rápido a señales de alta calidad y pueden responder con mayor celeridad a las actividades sospechosas identificadas por el sector privado.

Unas PPP más sólidas son esenciales para mejorar la comprensión de los riesgos emergentes del FT y las tipologías asociadas a las SMSP. La cooperación continua entre los SMSP, las entidades financieras reguladas y las entidades de CFT, así como las autoridades competentes, seguirá siendo fundamental para desarrollar medidas de mitigación coordinadas y eficaces. Entre las áreas clave de atención se incluyen el intercambio de información sobre tendencias emergentes y las mejores prácticas para presentar y gestionar las solicitudes de información, lo que permite una interrupción más eficiente y coordinada de las actividades de FT.

Mensaje clave: Una colaboración efectiva permite mitigar mejor los riesgos, al tiempo que respalda las operaciones comerciales legítimas.

Recomendaciones

5

El reto para la comunidad internacional no es la innovación en sí misma, sino garantizar que las nuevas soluciones financieras se desarrollen y apliquen de manera que sean resistentes al abuso, se basen en sólidas salvaguardias en materia de PLD/CFT cuando proceda, y se ajusten a un enfoque basado en el riesgo. Abordar el uso indebido de las SMSP con fines de terrorismo y FT requiere que las jurisdicciones eliminen la fragmentación institucional y refuercen tanto la coordinación interinstitucional a nivel nacional como la cooperación internacional entre las autoridades competentes implicadas en la detección, desarticulación, investigación y enjuiciamiento de las actividades de FT. La colaboración proactiva con las SMSP también contribuirá a desarrollar una visión común de los riesgos potenciales y las tendencias emergentes a medida que la tecnología siga evolucionando. Este esfuerzo debería involucrar no solo a las autoridades operativas, sino también a los responsables políticos y a los expertos jurídicos, para garantizar que las respuestas sigan siendo efectivas.

Reforzar el diálogo estructurado entre las autoridades competentes y el sector privado

Incluidas las SMSP, las IF y los PSAV, reconociendo sus funciones complementarias a la hora de identificar y detectar actividades terroristas y relacionadas con FT, de modo que las SMSP aportan visibilidad sobre los comportamientos observados en línea y los proveedores de servicios financieros rastrean la obtención y el movimiento de fondos.

Siempre que sea posible, se deben establecer marcos jurídicos que permitan un intercambio de datos oportuno y seguro entre las SMSP, las IF, los PSAV y las autoridades competentes, de conformidad con la normativa en materia de protección de datos y privacidad. Se anima a las autoridades competentes a proporcionar un contexto claro y específico para cada caso que respalde las solicitudes concretas, mientras que se anima a las SMSP —dentro de un marco seguro y predecible— a compartir información sobre los riesgos emergentes y las tendencias de actividades sospechosas identificadas a través de sus actividades de control.

Facilitar un intercambio efectivo de información y reforzar las PPP

Aclarar el ámbito de aplicación de la normativa

Seguir profundizando en el conocimiento de qué funcionalidades de las SMSP se ajustan a los Estándares del GAFI e identificar en qué casos se aplicarán las obligaciones en materia de PLD/CFT.

Evaluar de forma continua los riesgos de FT asociados a las tecnologías emergentes, incorporando los conocimientos especializados del sector privado en las evaluaciones de riesgos y mejorando la comprensión de las tendencias y tipologías en constante evolución (por ejemplo, la IA, las comunicaciones cifradas, los activos virtuales (AV), las finanzas descentralizadas (DeFi) y los pagos integrados).

Mejorar la comprensión del riesgo

Mejorar la coordinación entre organismos

Mejorar la colaboración entre las UIF, los organismos supervisores, las autoridades de aplicación de la ley (incluidas las unidades de antiterrorismo y CFT, así como las unidades cibernéticas) y los organismos de inteligencia.

Reforzar las capacidades para relacionar las operaciones financieras con el comportamiento en línea, los contenidos y las redes.

Vincular la inteligencia financiera y la inteligencia digital

Reforzar la cooperación internacional

Mejorar el acceso transfronterizo a las pruebas electrónicas y agilizar el uso de los mecanismos de cooperación jurídica.

Proporcionar formación especializada y herramientas para detectar e investigar el FT en los ecosistemas digitales.

Desarrollar la capacidad operativa

Elaborar indicadores específicos

Ampliar las tipologías y señales de alerta específicas del uso indebido de las SMSP (por ejemplo, lenguaje codificado, códigos QR, herramientas de monetización).

Evaluar los riesgos asociados a las donaciones, las retransmisiones en directo, las suscripciones, los ingresos publicitarios y las funcionalidades de financiamiento colectivo.

Mejorar la comprensión de las funciones de monetización

www.fatf-gafi.org