LAVADO DE ACTIVOS VIRTUALES EN EL PERÚ: REFORMAS URGENTES

DOI: https://doi.org/10.53870/lvj.387

Víctor Roberto Prado Saldarriaga [1]
Poder Judicial del Perú
https//orcid.org/0000-0002-7752-0640
vprado_2000@yahoo.com

RESUMEN
El presente artículo analiza las características actuales del delito de lavado de activos con empleo de criptomonedas o activos virtuales y los estándares internacionales para su prevención y control. Asimismo, se examinan las posibilidades de adaptación que tiene la legislación penal peruana a la represión penal de esa nueva modalidad delictiva. El autor concluye proponiendo algunas propuestas hermenéuticas y reformas legislativas; de esta manera, los tipos penales contenidos en el Decreto Legislativo 1106 podrán cumplir ese objetivo político criminal.

Palabras claves: Lavado de activos - activos virtuales - cibercriminalidad - reformas legales.

1. UN NUEVO PROBLEMA CRIMINAL: LAVADO DE ACTIVOS VIRTUALES

La definición más caracterizada de activos virtuales o criptomonedas es la que ha difundido el Grupo de Acción Financiera Internacional (GAFI), la cual precisa lo siguiente:

> Un activo virtual es una representación digital de valor que se puede comercializar o transferir digitalmente y se puede utilizar para pagos o inversiones. Los activos virtuales no incluyen representaciones digitales de moneda fiat, valores y otros activos financieros que ya están cubiertos en otras partes de las Recomendaciones del GAFI.

En un mundo globalmente virtualizado las ventajas operativas y de tráfico social que ofrecen la creación, emisión y empleo de activos virtuales (AV) son innegables

1 Abogado por la Universidad Nacional Mayor de San Marcos, Doctor en Derecho por la Universidad de Valencia – España, Juez Supremo Titular de la Corte Suprema de Justicia de la República del Perú y catedrático de Derecho Penal.

e imprescindibles. Ello explica su acelerado y extensivo impacto en los negocios y transacciones de naturaleza económica, bursátil o de intermediación financiera.

Ahora bien, la clave de ese crecimiento y positiva aceptación responde a una hábil estrategia de marketing que ha explotado eficientemente la condición intrínseca de los activos virtuales de ser un medio de pago cómodo, una alternativa menos costosa y con mayor rentabilidad que el dinero en efectivo. Además, los activos virtuales aminoran notablemente los riesgos de inseguridad ciudadana y de victimización hoy tan altos en las urbes latinoamericanas. Asimismo, han logrado una favorable inserción social entre la población regional por "la inalterabilidad y seguridad en su operación por lo que se pueden utilizar como medio de transferencia y acumulación de valor para los usuarios a costos bajos, comparados con el sistema financiero tradicional" (Redacción Gestión, 2019).

Pero también los activos virtuales suscitaron un expectante interés en la criminalidad organizada, sobre todo, porque las estructuras criminales identificaron en ellos una nueva ruta de posibilidades para el lavado de sus ganancias ilegales o contra su congelamiento, bloqueo o decomiso internacional. En efecto, la fácil portabilidad e, incluso, la impredecible volatilidad de estos nuevos activos los convertía en útiles "medios virtuales" para el eficiente aseguramiento de los capitales de origen ilícito. Además, sus diversas capacidades de intercambio y el hecho de no requerir intermediarios (Arango-Arango et al., 2018) harían más complejo y dificultoso "seguir la ruta del dinero" de procedencia criminal. Al respecto, cabe destacar que son tres las principales ventajas criminógenas que conlleva el uso delictivo de activos virtuales:

- El anonimato que aseguran a los operadores de las transacciones y a su beneficiario final.
- El alto grado de dificultad para el rastreo informático oportuno de las transacciones sospechosa en la inmensidad del ciberespacio.
- Una regulación normativa todavía insuficiente y no estandarizada sobre la creación, circulación y supervisión estatal de monedas virtuales y de las empresas dedicadas a su adquisición, intercambio o transferencia.

También es pertinente precisar que el proceso del lavado de activos virtuales se desarrolla con las mismas etapas o estaciones que tradicionalmente recorren las operaciones tradicionales del lavado de activos físicos de origen ilegal. Esto es, como explica AGUEDO, requiere también de actos de colocación, de intercalación (estratificación) y de integración. La autora citada describe el proceso y sus etapas del modo siguiente:

Colocación: Los criminales tienen la capacidad de abrir de manera rápida y anónima billeteras electrónicas desde donde pueden comprar monedas virtuales usando el dinero obtenido en actividades ilícitas.

Estratificación: Las oportunidades para llevar a cabo una cantidad innumerable de transacciones, de país en país, son múltiples. Con cada transferencia se va borrando la pista del origen real del dinero.

Integración: Cada vez son aceptadas como medios de pago en distintos establecimientos. También se da la posibilidad de que estos mismos delincuentes inviertan en negocios de criptomercados, tales como ICO (Initial Coin Offering) para la creación de nuevas criptomonedas (Aguedo, 2019).

En términos similares, la Financial Crime Academy (2024) grafica también el *modus operandi* del lavado de activos virtuales resaltando lo que acontece, generalmente, en cada una de sus tres fases:

Colocación: Los fondos ilegales se introducen en el sistema de criptomonedas a través de diversos medios como comprarlos en un intercambio, minarlos o recibirlos como pago por actividades ilícitas.

Estratificación: Implica una serie de transacciones destinadas a ocultar la propiedad de los fondos como convertirlos en diferentes criptomonedas, transferirlos a múltiples cuentas o utilizar servicios de mezcla que agrupan múltiples transacciones para ocultar el origen de los fondos.

Integración: Los fondos lavados se devuelven al sistema financiero legítimo como fondos aparentemente legales, ya sea vendiendo las criptomonedas por moneda fiduciaria o usándola para comprar bienes o servicios.

Por todas esas características y la preocupante eficiencia que demostraba tener el lavado de activos virtuales, se hicieron más constantes las clarinadas de alerta sobre estos riesgos de desvío delictivo durante el último quinquenio (SBS, 2019b, pp. 7-8). Por ejemplo, se comenzó a denunciar con insistencia el incremento subrepticio de su empleo en prácticas fraudulentas y de conversión o transferencia de capitales de origen ilegal (Pérez López, 2017, p. 187). Asimismo, las agencias oficiales contra la criminalidad organizada empezaron, también, a diseñar programas de especialización y adiestramiento para que sus operadores estuvieran en aptitud de descubrir y sancionar estos delitos virtualizados. Por ejemplo, se insistió en la urgencia de elaborar "materiales modelo que se puedan adaptar fácilmente para la formación de aspirantes, investigadores, expertos forenses, fiscales, jueces y otros" (Notes de Seguretat, 2023). Igualmente, el GAFI decidió tomarlos en cuenta a partir del 2015. Así, este organismo especializado en la prevención del lavado de activos informó a la comunidad financiera mundial

"que las monedas virtuales convertibles que se pueden cambiar por moneda real u otras monedas virtuales **son potencialmente vulnerables al abuso de lavado de activos y la financiación terrorista** por muchos motivos" (GAFI, 2015, p. 35). Asimismo, el GAFI puso de relieve que la modificación constante y la descentralización del soporte tecnológico de los activos virtuales complicaba su detección oportuna por las autoridades competentes y propiciaba la extensión continua de sus transacciones ilícitas en los circuitos del mercado virtual y, claro está, en la Darknet. Además, los activos virtuales de tipo criptomonedas "convertibles descentralizadas, que permiten transacciones de persona a persona de manera anónima, parecen existir en un universo digital totalmente fuera del alcance de cualquier país en particular" (GAFI, 2015, p. 35).

Este diagnóstico coincidía con lo opinado por expertos como Pérez López, quien, destacando la capacidad criminógena de los activos virtuales, señalaba "que el uso de criptomonedas supone una ampliación importante de la panoplia de posibilidades a disposición de los delincuentes". Asimismo, esta modalidad delictiva era "una de las opciones más interesantes para los blanqueadores y más disruptivas para su persecución (dada su sencillez, su eficacia en términos de costes en comparación con otros métodos y las dificultades técnicas asociadas a su trazado y evitación por las autoridades)" (Pérez López, 2017, pp. 152-155). Por su parte, otros especialistas graficaron la potencialidad criminógena de las criptomonedas y daban a conocer listados de tipologías, a través de las cuales era posible materializar operaciones de **lavado de activos con empleo de criptomonedas.** De las cuales, las más utilizadas eran las siguientes:

- Realización de múltiples transacciones de alto valor en una sucesión corta, por ejemplo, dentro de un período de 24 horas.
- Activación de importante volumen de transacciones de diferentes clientes enviadas hacia y desde la dirección de la billetera, con monedas virtuales convertibles, que no se observa como algo habitual y conocido.
- Transferencias de Activos Virtuales inmediatamente a múltiples proveedores de servicios de activos virtuales, especialmente a registrados u operados en otra jurisdicción donde no existe relación con el lugar donde el cliente vive o realiza negocios; o la regulación AML/CFT/PF es inexistente o débil.
- Depósitos de Activos Virtuales, en un intercambio, para efectuar el retiro inmediatamente sin actividad de intercambio o adicional a otros Activos Virtuales; convertirlo en múltiples tipos de Activos Virtuales; o retirarlos inmediatamente mediante una billetera de privacidad.
- Aceptar depósitos de fondos sospechosos de ser robados o depositar fondos fraudulentos de direcciones de Activos Virtuales que han sido identificadas

como tenedoras de fondos robados, o en direcciones vinculadas a los tenedores de fondos robados.
- La intervención de las denominadas "mulas electrónicas" quienes practicaron actos de conversión de dinero fiat en activos virtuales que luego transfieren a las billeteras electrónicas de los verdaderos dueños de aquellos fondos de origen ilícito (Santiago Gonzáles, 2021).

Con posterioridad al dramático episodio de la pandemia de la COVID-19 y con la experiencia criminológica y criminalística acumulada durante esta grave coyuntura, el GAFI fue difundiendo también señales de alerta vinculadas a operaciones con activos virtuales y a quienes las ejecutaban o se benefician de ellas. Para una mejor ilustración transcribimos las más importantes.

Señales de alerta relacionadas con las operaciones

Si bien los AV aún no son ampliamente utilizados por el público, su uso s e ha popularizado entre los criminales. Su uso para propósitos de LD surgió por primera vez hace más de una década, pero se están volviendo cada vez más comunes para la actividad delictiva en general. Este conjunto de indicadores demuestra cómo las señales de alerta tradicionalmente asociadas con operaciones que involucran medios de pago más convencionales siguen siendo relevantes para detectar posibles actividades ilícitas relacionadas con los AV.

Tamaño y frecuencia de las operaciones

- Estructurar operaciones de AV (por ejemplo, cambios o transferencia) en pequeñas cantidades, o en cantidades por debajo de los umbrales de mantenimiento de registros o informes, similar a estructurar operaciones en efectivo.
- Realizar múltiples operaciones de alto valor:
  - en una sucesión breve, como en un período de 24 horas;
  - en un patrón escalonado y regular, sin más operaciones registradas durante un largo periodo posterior, lo cual es particularmente común en casos relacionados con *ransomware*;
  - a una cuenta recién creada o previamente inactiva.
- Transferir AV inmediatamente a múltiples VASP, especialmente a VASP registrados u operados en otra jurisdicción donde:
  - no hay relación con el lugar donde vive o realiza negocios el cliente;
  - regulación PLD/CFT inexistente o débil.
- Depositar los AV en una oficina de cambios y luego, a menudo, inmediatamente:

  - retirarlos sin actividad de cambios adicional a otros, lo cual es un paso innecesario e incurre en tarifas de operación;
  - convertirlos en múltiples tipos de AV, incurriendo nuevamente en tarifas de operación adicionales, pero sin una explicación comercial lógica (por ejemplo, diversificación de la cartera);
  - retirarlos AV de un VASP inmediatamente a una cartera privada. Esto convierte efectivamente el intercambio / VASP en una mezcla para el LD.
- Aceptar recursos sospechosos de ser robados o fraudulentos:
  - depositar recursos de direcciones de AV que han sido identificadas como tenedoras de fondos robados, o direcciones vinculadas a los tenedores de fondos robados.

Señales de alerta relacionadas con el anonimato

Este conjunto de indicadores se basa en las características inherentes y las vulnerabilidades asociadas con la tecnología subyacente de los AV. Las diversas características tecnológicas aumentan el anonimato y agregan obstáculos a la detección de actividades delictivas por parte de las LEA. Estos factores hacen que los AV sean atractivos para los criminales que buscan disfrazar o almacenar sus recursos. Sin embargo, la mera presencia de estas características en una actividad no sugiere automáticamente una operación ilícita. Por ejemplo, el uso de *hardware* o una cartera de papel puede ser legítimo como una forma de proteger a los asistentes virtuales contra robos.

Nuevamente, la presencia de estos indicadores debe considerarse en el contexto de otras características sobre el cliente y la relación, o una explicación comercial lógica.

- Operaciones de un cliente que involucran más de un tipo de AV, a pesar de tarifas de operación adicionales, y especialmente aquellos que brindan mayor anonimato, como criptomonedas o monedas privadas.
- Mover un AV que opera en una cadena de bloques pública y transparente, como Bitcoin, a un intercambio centralizado y luego intercambiarlo inmediatamente por una criptomoneda de anonimato o moneda privada.
- Clientes que operan como un VASP no registrado / sin licencia en sitios web de intercambio *peer-to-peer* (P2P), particularmente cuando existe la preocupación de que manejen un mayor número de transferencias AV en nombre de su cliente y le cobren tarifas más altas que la transmisión de servicios ofrecidos por otros cambios. Uso de cuentas bancarias para facilitar estas operaciones P2P.

- Actividad transaccional anormal (nivel y volumen) de AV cobrados en intercambios de carteras asociadas a la plataforma P2P sin una explicación comercial lógica.
- AV transferidos hacia o desde carteras que muestran patrones previos de actividad asociados con el uso de VASP que operan servicios de mezcla o caída o plataformas P2P.
- Operaciones que hacen uso de servicios de mezcla y rotación, lo que sugiere la intención de ocultar el flujo de recursos ilícitos entre direcciones de carteras conocidas y mercados de redes oscuras.
- Recursos depositados o retirados de una dirección o cartera de AV con enlaces de exposición directa e indirecta a fuentes sospechosas conocidas, incluidos mercados negros, servicios de mezcla / volteo, sitios de apuestas cuestionables, actividades ilegales (por ejemplo, *ransomware*) y / o informes de robo.
- Uso de carteras de papel o *hardware* descentralizadas / no alojadas para transportar AV a través de las fronteras.
- Usuarios que ingresan a la plataforma VASP tras registrar sus nombres de dominio de Internet a través de *proxies* o registradores de nombres de dominio que suprimen o censuran a los propietarios de los nombres de dominio.
- Usuarios que ingresan a la plataforma VASP mediante una dirección IP asociada con una red oscura u otro *software* similar que permite la comunicación anónima, incluidos correos electrónicos cifrados y VPN.
- Operaciones entre socios que utilizan varios medios de comunicación anónimos encriptados (por ejemplo, foros, chats, aplicaciones móviles, juegos en línea, etc.) en lugar de un VASP.
- Un alto número de carteras AV aparentemente no relacionadas controladas desde la misma dirección IP (o dirección MAC), lo que puede implicar el uso de carteras shell registradas para diferentes usuarios para ocultar su relación entre ellos.
- Uso de AV cuyo diseño no está adecuadamente documentado, o que están vinculados a posibles fraudes u otras herramientas destinadas a implementar esquemas fraudulentos, como los esquemas Ponzi.
- Recibir o enviar recursos a los VASP cuyos procesos de DDC o conocimiento de su cliente son débiles o inexistentes.
    - Uso de cajeros automáticos / quioscos AV: o a pesar de las tarifas de operación más elevadas e incluidas las que suelen utilizar las mulas o las víctimas de estafas; o en lugares de alto riesgo donde ocurren más actividades delictivas.

- El uso de un cajero automático o quiosco no es suficiente en sí mismo para constituir una señal de alerta, pero lo sería si se combinara con la máquina en un área de alto riesgo o se usara para operaciones pequeñas repetidas (u otros factores adicionales).

Respecto a la experiencia peruana, los funcionarios de la UIF-Perú han informado que las modalidades de conversión delictiva de activos virtuales que se han detectado en el país son aún muy básicas. Por ello, cuando se viabilizan con intervención de canales de la intermediación financiera su detección y rastreo se facilitan, por lo que posibilita el oportuno congelamiento de los fondos involucrados en la transacción delictiva:

Se ha identificado que el dinero mal habido termina siendo usado para la compra de criptomonedas. En alguna oportunidad se compraron criptoactivos a una empresa peruana, que vendía criptomonedas, y pudimos congelarlos. La UIF tiene la facultad de congelar el dinero cuando se tiene la certeza de que el dinero tiene un origen ilícito. (…) Se vuelve vulnerable a los ojos de la UIF cuando pasa al sistema financiero. Cuando encontramos el dinero en el sistema financiero, una herramienta que tenemos (para evitar su uso) es que podemos congelarlo para asegurarnos de que esté en manos de las autoridades hasta concluir la investigación. Al final se puede incautar (Guardia Quispe, 2023).

No cabe duda, pues, que hoy concurrimos a una etapa expectante donde se pugna por demostrar y aceptar que el uso lícito e ilícito de los activos virtuales es un componente más de la realidad económica actual y que lo será también en el futuro inmediato. Por consiguiente, las políticas y programas sobre desarrollo socioeconómico o financiero que formulen los Estados en los años siguientes tienen necesariamente que tomar en cuenta la presencia de los activos virtuales y de los negocios que con ellos se realizan. Estos, obviamente, no estarán exentos de su desviación y uso criminal. Por consiguiente, su adecuada regulación en el presente se ha de convertir también en un estándar más de garantía y acreditación de todo programa estratégico de seguridad o de gobierno digital que diseñen e implementen los Estados. Al respecto, cabe destacar que los países desarrollados han logrado notables avances en este proceso. Un ejemplo relevante de ese proceder prospectivo ha sido la elaboración y aplicación de pertinentes protocolos para la supervisión reforzada o el control tributario de los activos virtuales, así como para el registro de su propiedad, tenencia y transferencias (SBS, 2019a).

Ahora bien, el sofisticado y renovado *modus operandi*, para el blanqueo de ganancias ilícitas que hemos descrito, se ha visto reforzado a través de los eficientes procedimientos y técnicas de ofuscación o disfraz que ofertan las organizaciones

criminales dedicadas al lavado de activos virtuales en la Darknet. Efectivamente, entre ellas detectan, sobre todo, la aplicación de programas de mezclado de criptomonedas y de encriptación temporal reforzada, los cuales han potenciado la imposibilidad del rastreo de las operaciones y la sólida desvinculación de los usuarios, beneficiarios y proveedores de estos servicios ilegales. Además, han surgido nuevas criptomonedas, como monero, que han potenciado también su imposibilidad de rastreo y de vinculación de las transacciones lícitas e ilícitas. También, en la web oscura hoy es posible el reclutamiento masivo de "cibermulas", las que a modo de "pitufos virtuales" ejecutan con las ganancias ilegales que les suministran los grupos criminales múltiples operaciones en cortos periodos de tiempo a través de la amplitud del ciberespacio. Sobre estas redobladas capacidades blanqueadoras de los activos virtuales, un informe del 2023 de EUROPOL ha detectado lo siguiente:

Los ciberdelincuentes implicados en ciberataques y servicios relacionados, así como los que comercian y administran mercados de la web oscura, realizan sus transacciones financieras casi exclusivamente en criptomonedas. por esta razón, hacen un amplio uso de técnicas de ofuscación para anonimizar sus actividades financieras antes de cobrar los beneficios ilícitos. estas técnicas incluyen el uso de mezcladores, intercambiadores, operaciones extrabursátiles e intercambios descentralizados (...). Todos los tipos de ciberdelincuentes utilizan mulas de dinero para blanquear beneficios ilícitos, ya sea en dinero fiduciario o en criptomonedas. las mulas de dinero son facilitadores clave para el blanqueo de los beneficios ilícitos generados por la ciberdelincuencia, ya que permiten a los delincuentes rápidamente mover fondos a través de una red de cuentas, a menudo en diferentes países (IOCTA, 2023).

Por consiguiente, poder penetrar, descubrir o desmezclar las operaciones de lavado de activos virtuales exige también una nueva cibercriminalística, que recién en los últimos tres años ha comenzado a aplicarse y difundirse entre las agencias especializadas del sistema penal. Un ejemplo de los esfuerzos por superar estas necesidades operativas es la Guía de investigación en el lavado de activos mediante criptodivisas, difundida por El Pacto Europa-Latinoamérica. Según la síntesis introductoria de dicho manual, se abordan, entre otros, los siguientes aspectos de utilidad criminalística:

Se procederá a describir y definir las criptodivisas, los diferentes actores involucrados para su obtención, su uso, trazabilidad y, lo más relevante en el aspecto que nos ocupa, las distintas metodologías utilizadas para llevar a cabo actividades de blanqueo de capitales. Describiremos los elementos utilizados para la facilitación del lavado de activos con criptomoneda, sus vulnerabilidades, así como distintos aspectos en relación con las monedas virtuales, independientemente de

la legislación aplicable. Para afrontar el reto que supone la investigación policial de cualquier modalidad delictiva que incluye el uso de criptoactivos es preciso realizar ciertas adaptaciones en las estructuras policiales que permitan reaccionar de forma adecuada ante esta amenaza. Veremos ciertas recomendaciones y buenas prácticas sobre este aspecto (Bodoque Agredano. Orduna Lanau, 2022, p.7).

2. ESTRATEGIAS INTERNACIONALES DE PREVENCIÓN Y CONTROL

Cabe recordar que hacia finales del siglo XX se configuró el primer espacio internacional contra el lavado de activos mediante la aprobación de la Convención de las Naciones Unidas contra el Tráfico Ilícito de Estupefacientes y Sustancias Psicotrópicas en 1988 (Prado Saldarriaga, 1997). Posteriormente. ya en la primera década del siglo XXI, se fueron configurando otros espacios globales similares contra la criminalidad organizada transnacional (Convención de Palermo de 2001) y contra la corrupción (Convención de Mérida de 2003), donde se incluyeron estrategias y medidas específicas para la prevención y represión penal de las operaciones de lavado de activos (Prado Saldarriaga, 2019). Próximamente culminarán los trabajos del Proyecto de la Convención Internacional contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos, donde también, a iniciativa de la delegación peruana, quedará diseñada un nuevo espacio internacional para la persecución y sanción de los actos de lavado que se realicen con empleo de activos virtuales[2]. De allí, pues, que resulte pertinente y oportuno analizar el surgimiento y desarrollo de los estándares internacionales que en el presente se relacionan con la prevención, el tratamiento penal y la cooperación internacional contra la amenaza criminal del lavado de activos virtuales.

Al respecto, cabe mencionar, inicialmente, que la oportuna constatación empírica de todos aquellos riesgos, amenazas y *modus operandi* sofisticado, que caracterizan e identifican a las tipologías delictivas del lavado de activos virtuales, fueron perfilando también la definición de objetivos y estrategias de política criminal internacional para prevenir, controlar e interdictar eficazmente sus manifestaciones en el ciberespacio. En ese contexto, por ejemplo, se establecieron los siguientes tres objetivos esenciales:

1. Preservar la integridad del sistema financiero salvaguardándolo del lavado de activos virtuales o de conductas delictivas análogas de financiación del terrorismo.

2 En el artículo 2 de este proyecto, luego de arduos debates, la delegación peruana logró que se incluya como un nuevo objeto de acción del delito a los activos virtuales.

2. Desarrollar una tutela preventiva eficiente para los proveedores y consumidores honestos de activos virtuales.
3. Regular el control tributario y contable de todo tipo de activos virtuales, obligando a sus usuarios o proveedores a cumplir con regímenes de registro de sus transacciones.

Un primer aporte técnico para viabilizar todas esas metas y medidas fue la aprobación el año 2019 de la Nota Interpretativa de la Recomendación N°15 sobre Nuevas Tecnologías[3] del GAFI. En este documento se introdujeron lineamientos específicos que ayudarían a configurar una legislación especializada y a configurar procedimientos eficaces para la prevención, control y sanción de las operaciones o transacciones ilícitas que se ejecuten con el empleo de "activos virtuales (AV)". Por ejemplo, se sugirió la elaboración y aplicación de instrumentos de supervisión, así como de técnicas de registro de los "proveedores de servicios de activos virtuales (PSAV)". También se insertaron recomendaciones para la implementación eficiente de medidas de cooperación interestatal contra las operaciones ilícitas con activos virtuales. Igualmente, se estableció como obligación de los países el incorporar en su derecho interno sanciones penales o administrativas que fueran idóneas y proporcionales para reprimir los delitos con activos virtuales o las infracciones a los regímenes de registro y supervisión preventiva (GAFILAT, 2018b, pp. 77-79). Entre las principales recomendaciones y disposiciones formuladas cabe mencionar las siguientes:

- Los países deben considerar los activos virtuales como "bienes", "productos", "fondos", "fondos y otros activos" u otros activos de valor equivalente. Los países deben aplicar las medidas pertinentes en virtud de las recomendaciones del GAFI a los activos virtuales y a los proveedores de servicios de activos virtuales (PSAV).
- Los países deben identificar, evaluar y comprender los riesgos de lavado de activos y financiamiento del terrorismo que surgen de las actividades de activos virtuales y las actividades u operaciones de los PSAV.
- Los países deben exigir que los PSAV identifiquen, evalúen y tomen medidas eficaces para mitigar sus riesgos de lavado de activos y financiamiento del terrorismo.
- Los PSAV deben tener licencia o registrarse, como mínimo, en la(s) jurisdicción(es) donde se crean. En los casos en que el PSAV sea una persona

3 El texto de la 15° recomendación y su nota interpretativa pueden verse en GAFI (2021a), pp.106-108.

física, se le debe exigir que esté autorizado o registrado en la jurisdicción donde se encuentra su lugar de negocios. Las jurisdicciones también pueden requerir que los PSAV, que ofrecen productos y/o servicios a los clientes en su jurisdicción o que realizan operaciones desde su jurisdicción, tengan licencia o estén registrados en esta jurisdicción.

- Los países deben garantizar que los PSAV estén sujetos a una reglamentación y supervisión o monitoreo adecuados de ALA/CFT y que estén aplicando eficazmente las recomendaciones pertinentes del GAFI, a fin de mitigar los riesgos de lavado de activos y financiamiento del terrorismo que surgen de los activos virtuales.
- Los países deben asegurarse de que exista una serie de sanciones efectivas, proporcionadas y disuasorias, ya sean penales, civiles o administrativos, disponibles para hacer frente a los PSAV que no cumplen los requisitos ALA/CFT. Las sanciones deben aplicarse no solo a los PSAV, sino también a sus directores y directivos jerárquicos.
- Los países deben proporcionar rápida, constructiva y eficazmente la mayor gama posible de cooperación internacional en relación con el lavado de activos, los delitos determinantes y el financiamiento del terrorismo en relación con los activos virtuales.

Posteriormente, en el año 2021, el GAFI detalló, con mejor especificación, la implementación operativa de tales lineamientos a través de la Guía Actualizada para un enfoque basado en el riesgo. Activos Virtuales y Proveedores de Servicios de Activos Virtuales (GAFI, 2021). Sobre la finalidad funcional de dicho documento se destacó lo siguiente:

La Guía busca explicar cómo deben aplicarse las Recomendaciones del GAFI a las actividades de AV y a los PSAV; proporciona ejemplos, cuando son relevantes o potencialmente más útiles; e identifica los obstáculos para aplicar las medidas de mitigación junto con las posibles soluciones. Pretende servir de complemento a la R.15 y a su NIR 15 que describen toda la gama de obligaciones aplicables a los PSAV, así como a los AV, en virtud de las Recomendaciones del GAFI, incluidas las Recomendaciones relativas a los "bienes", "productos", "fondos", "fondos u otros activos" y otros "valores equivalentes". De este modo, la Guía apoya la aplicación efectiva de las medidas nacionales ALA/CFT para la regulación y supervisión de los PSAV (así como de otros sujetos obligados) y de las actividades cubiertas de los AV en las que participan, así como el desarrollo de un entendimiento común de lo que implica un EBR en materia ALA/CFT (GAFI, 2021, pp. 8-9).

Sin embargo, en un primer estudio de evaluación que realizaron los expertos del GAFI, se pudo constatar que los países vinculados a sus recomendaciones

habían avanzado muy poco en la implementación de la 15° recomendación y de su nota interpretativa. Es más, eran pocos los países que habían hecho efectivo el mandato de incluir expresamente en el derecho interno disposiciones legales sobre la "regla de viaje". Esto es, la aplicación de formas espontaneas de cooperación que permitirían la obtención y el intercambio de información pertinente desde los PSAV sobre el beneficiario y el generador de una transacción con activos virtuales. Por tal razón, el mes de junio de 2022 el GAFI publicó un nuevo instrumento correctivo y de exhortación "Actualización sobre la implementación de los estándares del GAFI acerca de los activos virtuales y prestadores de servicios". En dicho documento se demandó a los países, entre otros requerimientos el cumplimiento efectivo de las siguientes medidas:

- Tanto los miembros del GAFI como los integrantes de los cuerpos regionales tipo GAFI deberán acelerar el cumplimiento de la R15 y su nota interpretativa.
- Los países que no han introducido la regla de viaje en su legislación deberán hacerlo lo más pronto posible. Asimismo, los países miembros del GAFI deberán compartir sus experiencias y buenas prácticas en la materia.
- Tanto los PSAV como el sector privado deberán reforzar acciones para facilitar la interoperabilidad de la regla de viaje, por medio de soluciones tecnológicas que aseguren flexibilidad para su implementación, de conformidad con los requerimientos de cada jurisdicción.
- En relación con los mercados y las nuevas tendencias, tanto el GAFI como los PSAV deberán continuar monitoreando a fin de establecer si se requieren más esfuerzos del primero para determinar la forma en que los estándares se aplican a las DEFI u los NFT con base en el enfoque basado en riesgo. De igual manera, el GAFI se compromete a trabajar con sus miembros para generar conciencia sobre las tendencias comunes de los pagos de Ransomware y el lavado de activos relacionado por medio de AV y PSAV (FATF, 2022, pp. 17-22).

Paralelamente, con similares propósitos, el GAFI suministró también a los países que lo integran un listado detallado de señales de alerta. Las que ayudarán a las agencias de prevención y control penal a lograr una lectura técnico-criminalística más homogénea sobre los ROS vinculados a operaciones de lavado con activos virtuales. El propósito operativo de este didáctico instructivo se sintetizo en los siguientes párrafos:

1. Los Activos Virtuales (AV) y los servicios relacionados tienen el potencial de

estimular la innovación y la eficiencia financiera, pero sus características distintivas también crean nuevas oportunidades para que los lavadores de dinero, los financiadores del terrorismo y otros criminales laven sus ganancias o financien sus actividades ilícitas. La capacidad de realizar operaciones transfronterizas rápidamente no solo permite a los criminales adquirir, mover y almacenar activos digitalmente, a menudo fuera del sistema financiero regulado, pero también disfrazar el origen o destino de los recursos y dificultar que los sujetos obligados identifiquen las actividades sospechosas de manera oportuna. Estos factores añaden obstáculos a la detección e investigación de la actividad criminal por las autoridades nacionales.

4. Las agencias operativas, incluidas las Unidades de Inteligencia Financiera (UIF), las autoridades de procuración de justicia (LEA, por sus siglas en inglés) y los fiscales pueden encontrar este informe como una referencia útil para analizar los Reportes de Operaciones Sospechosas (ROS) o mejorar la detección, investigación y aseguramiento de los AV involucrados en el uso indebido (FATF, 2020).

Como se indicó, en dicho documento se incluyó también un nutrido listado de nuevas señales de alerta. Las que deberían tener en cuenta los operadores del sistema antilavado para poder identificar e interdictar oportunamente las potenciales operaciones de lavado de activos virtuales. Por lo demás, para facilitar su comprensión y asimilación, estas señales de alerta fueron debidamente sistematizadas en base a indicadores y características de operaciones inusuales ejecutadas con activos virtuales. En ese sentido, se agruparon las señales de alerta por segmento, tipo de operación o rasgos inusuales. El listado elaborado quedo integrado por 6 segmentos que son los siguientes:

- Señales de alerta relacionadas con las operaciones.
- Señales de alerta relacionadas con los patrones de operación.
- Señales de alerta relacionadas con el anonimato.
- Señales de alerta sobre remitentes y beneficiarios.
- Señales de alerta en la procedencia de recursos o patrimonio.
- Señales de alerta relacionadas con riesgos geográficos (FATF, 2020b).

Ahora bien, la experiencia latinoamericana en políticas y estrategias de prevención y control del lavado de activos virtuales es mucho más reciente y se vincula con los esfuerzos desplegados en este dominio por el Grupo de Acción Financiera para Latinoamérica (GAFILAT) desde el año 2018. Este organismo

técnico regional, por ejemplo, realizó una primera aproximación estratégica a la problemática regional del lavado de activos virtuales durante el Ejercicio Bienal 2017-2018 de Tipologías Regionales realizado en Quito. En aquella ocasión se exhibieron dos tipologías delictivas relacionadas con el tráfico de bitcoins (GAFILAT, 2018a, pp. 79-80). Años después, en agosto de 2021, el GAFILAT desarrolló también un encuentro virtual de debate sobre esta materia y en diciembre del mismo año difundió en el Informe de Tipologías Regionales de LA/FT 2019-2020 un nuevo caso que mostraba la adquisición de activos virtuales a través de PSVA para operaciones de intercalación realizadas por tratantes de personas (GAFILAT, 2021, p. 110). No obstante, lo más relevante de estos primeros acercamientos es que ellos pusieron en evidencia que en nuestra región el empleo delictivo de activos virtuales utilizaba aún tipologías básicas y poco sofisticadas. Sin embargo, no dejaban de ser útiles y eficientes para el objetivo criminal de perderle el rastro a las ganancias ilícitas, sobre todo por la convergencia de factores estructurales propios de los países latinoamericanos. Por ejemplo, la paradójica composición de sus economías mayormente de condición emergente-informal constituía un sensible caldo de cultivo para esta nueva tipología criminal, pero, también, las manifiestas desigualdades de conectividad y desarrollo tecnológico que concurrían en cada país. Asimismo, se hicieron visibles notables limitaciones y deficiencias entre las agencias y los sistemas nacionales de control y supervisión. Esto último producía una brecha importante para la cooperación internacional afectando la eficacia y la factibilidad de ejecutar operativos virtuales combinados y transfronterizos. Atendiendo a todas aquellas brechas, disfunciones y deficiencias operativas que hemos enunciado, el GAFILAT, entre los años 2021-2023, se dedicó a elaborar y difundir importantes guías e instructivos con lineamientos y protocolos de prevención, investigación criminal y procesamiento penal de delitos de lavado de activos virtuales. Uno de estos documentos fue la *Guía sobre aspectos relevantes y pasos apropiados para la investigación, identificación, incautación y decomiso de activos virtuales*, publicada en 2021. La finalidad común de estos documentos técnicos era promover la armonización legislativa y lograr una capacitación estandarizada entre los operadores de las agencias nacionales competentes para la investigación, juzgamiento y sanción de los hechos punibles cometidos con criptomonedas. En estos manuales, además, no solo se ofrecían información teórica y práctica sobre la prevención y control del lavado de activos virtuales, sino, también, se recopilaban y daban a conocer las buenas prácticas y experiencias exitosas que ocurrían en la realidad latinoamericana durante la investigación e interdicción de tales delitos.

Concurrimos, pues, en Latinoamérica, a una etapa de intensificación de los procesos de producción legislativa para la prevención y control de los delitos de

lavado de activos virtuales. Los países de nuestro entorno regional han comenzado a adaptar sus sistemas jurídicos internos a la exigencias y recomendaciones formuladas en los estándares internacionales establecidos sobre la materia, como ha ocurrido en Argentina (2023), Brasil (2022), Colombia (2021) y Chile (2022). Por lo demás, la situación del sistema jurídico peruano en este dominio no es diferente y a ella queremos referiremos a continuación.

3. SOBRE EL CASO PERUANO

Aceleradamente el Perú se ha ido convirtiendo en el tercer país de la región con mayor volumen de transacciones con activos virtuales. Asimismo, en su territorio se están registrando y extendiendo nuevas manifestaciones de criminalidad organizada como la pesca ilegal, el tráfico ilegal de especies de flora y fauna silvestres, la inmigración ilegal y la tala forestal ilícita, las cuales requieren de innovadoras opciones de aseguramiento de sus ganancias ilícitas como las que les ofrece el lavado de activos virtuales (Observatorio Nacional de Política Criminal, 2021, 2022a). Además, en un detallado estudio promovido por la Superintendencia de Banca, Seguros y AFP, se ha revelado un largo listado de riesgos latentes de lavado de activos virtuales en el país (SBS, 2019a). En efecto, según las conclusiones de dicha investigación, son riesgos y amenazas considerables los siguientes:

- No existe una delimitación clara del ámbito de supervisión entre las organizaciones reguladores locales en el Perú.
- No existen marcos ALA / CFT para los PSAV en el Perú (incluyendo el requisito de un sistema de prevención del LA/FT documentado, procesos de DDC, etc.)
- No existen requisitos de registro o licenciamiento de los PSAV.
- No hay revelación de riesgo obligatoria ni requisitos justos hacia los clientes.
- No hay capacidad para monitorear las transacciones que ocurren con individuos o entidades corporativas con sede en el Perú.
- Riesgo de fraude y falsos esquemas de inversión.
- Riesgo de transacciones de OIM no reguladas y fraudulentas.
- Riesgos tecnológicos como piratería de claves privadas, etc.

Además, según las mismas fuentes oficiales, en la práctica de operaciones con activos virtuales en el Perú predominan las siguientes características:

Se cree que la mayoría de las transacciones son transacciones simples que utilizan tokens de pago. En su forma más simple, el flujo involucra a un individuo privado que compra un token de pago usando soles o dólares estadounidenses

de una cuenta bancaria, usando el token de pago para pagar a un tercero, y ese tercero retiene el token de pago o lo convierte de nuevo en una moneda fiduciaria. Hasta la fecha del informe realizado por True North Partners no identificaron ninguna transacción de OIM en Perú.

Dada la naturaleza informal y no regulada del mercado actual, no fue posible cuantificar con precisión los principales usos y flujos de AVs en el Perú hoy día (…). Esto indica que la necesidad de regulación y supervisión dentro del mercado peruano es fuerte, al menos en un nivel básico que cubre la ley de ALA, CFT, impuestos y valores (en términos de este último, dado que la mayoría de los AVs en Perú son tokens de pago y SMV se centrará en los tokens de activos, se estima que el impacto en el mercado de valores será limitado a corto y mediano plazo) (SBS, 2019a, p. 76).

Sin embargo, hay que tener en cuenta, igualmente, la concurrencia de otros factores de coyuntura como la actual crisis política, la inflación, la recesión económica y el continuo crecimiento de la informalidad (Cuadros, 2022), los cuales promueven la expansión del mercado de activos virtuales en territorio nacional. Por consiguiente, cabe inferir que todos esos indicadores y procesos económicos o políticos disfuncionales generan condiciones favorables para la extensión de operaciones de lavado con activos virtuales. Además, en dicho contexto el flujo de transacciones sin criptoactivos involucra a un mayor número de sectores y agentes económicos. Esto también se ve reflejado en la información suministrada por la Unidad de Inteligencia Financiera del Perú, la cual ha detectado que entre los años 2019 y abril 2022 la operatividad de lavado de activos virtuales se ha potenciado y diversificado en el país[4]. Asimismo, a ese estado de cosas cabe agregar las limitaciones criminalísticas y operativas que todavía evidencian las agencias estatales competentes para la detección e investigación temprana de operaciones de lavado con activos virtuales. Por ejemplo, el cuadro siguiente aporta un dato relevante sobre las características actuales del problema analizado: el variado espacio de las personas jurídicas y actividades económicas reportadas por operaciones y transacciones sospechosas con activos virtuales. Además, resalta el amplio espectro de la informalidad que aparece cubierto bajo un equívoco rubro económico "no determinado".

4 Nuestro reiterado agradecimiento al Dr. Sergio Espinosa Chiroque, superintendente adjunto de la Unidad de Inteligencia Financiera, por la información y cuadros estadísticos brindados y que aquí reproducimos.

Personas jurídicas reportadas por operaciones sospechosas con activos virtuales según su actividad económica 2019 – abril 2022

Sector económico	Número de personas jurídicas reportadas
Actividades inmobiliarias, empresariales y de alquiler	31
Intermediación financiera	9
Otras actividades de servicios comunitarios, sociales y personales	8
Comercio al por mayor y al por menor; reparación de vehículos automotores, motocicletas, efectos personales y enseres domésticos	6
Industrias manufactureras	2
Transporte, almacenamiento y comunicaciones	2
No determinado	29
Total	87

Fuente: UIF (2022)

No obstante, otro hallazgo importante que aporta el cuadro siguiente radica en que entre las personas jurídicas reportadas por operaciones o transacciones sospechosas el mayor nivel de frecuencias corresponde a personas jurídicas con menos de un año de creación. Este añade la sensible tendencia a la constitución y empleo de personas jurídicas de fachada en la práctica del lavado de activos virtuales en el país.

Personas jurídicas reportadas por operaciones sospechosas con activos virtuales según antigüedad de creación 2019 – abril 2022

Antigüedad de creación en años	Número de personas jurídicas reportadas
Menor a 1	29
Entre 1 y 3	10
Entre 4 y 5	14
Entre 5 y 10	3
Mayor a 10	2
No determinado	29
Total	87

Fuente: UIF (2022)

4. REFORMAS URGENTES EN LA LEGSLACIÓN PENAL

De acuerdo con los informes que hemos recibido hacia marzo de 2022, las unidades especializadas de la Policía Nacional, del Ministerio Público y del Poder Judicial reportaban que aún no contaban con investigaciones y procesos en trámite o concluidos por delitos de lavado de activos virtuales. Luego, hacia finales de febrero de 2023, se comunicó que ya estaban tramitándose algunos casos de investigaciones por lavado de activos virtuales en el Ministerio Público (Prado Saldarriaga, 2023, p. 343). Siendo así, una lectura prospectiva permite avizorar que en los próximos años la frecuencia de procesos penales por aquel delito se hará más constante, visible y sensible entre las unidades del sistema penal nacional. Por consiguiente, de cara a ese inminente futuro, resulta pertinente y oportuno medir la capacidad de adaptación de las operaciones o transacciones que configuren actos de lavado de activos virtuales a los delitos que regula el Decreto Legislativo 1106. Sobre todo, teniendo en cuenta que entre el nutrido bloque de decretos legislativos que se promulgaron hacia finales del 2023 y que reformaron o extendieron la legislación penal nacional, no se incluyeron modificaciones a los tipos penales del delito de lavado de activos y menos aún se hicieran referencias particulares al caso de los delitos de lavado con activos virtuales.

Al respecto, cabe recordar que en el Decreto Legislativo 1106 coexisten tres tipos penales nucleares que criminalizan el delito de lavado de activos en general. Asimismo, se incluyen dos modalidades de delitos periféricos, de las cuales la

composición actual de todos esos delitos es la siguiente:

- Los actos de conversión y transferencia de activos de origen ilegal se encuentran tipificados en el artículo 1°.
- Los actos de ocultamiento y tenencia de activos de origen ilegal son reprimidos por el artículo 2°.
- Los actos de trasporte, ingreso o egreso de dinero en efectivo o instrumentos financieros negociables al portador de origen ilegal están criminalizados en el artículo 3°.
- Los delitos periféricos de omisión de reporte de transacciones sospechosas y de rehusamiento, retardo o falsedad de información se hallan regulados en los artículos 5° y 6°, respectivamente.

Ahora bien, la actual morfología de tipos penales, que corresponden al delito de lavado de activos, debe abordarse tres problemas dogmáticos. El primero es estrictamente hermenéutico y consiste en esclarecer si las criptomonedas o activos virtuales pueden ser considerados objeto de acción de los delitos tipificados en los artículos 1°, 2° y 3° del Decreto Legislativo 1106. El segundo problema es esencialmente práctico y radica en verificar la flexibilidad de tales tipos penales para poder asimilar en sus alcances a las modalidades frecuentes de lavado de activos virtuales y que vienen ocurriendo en la realidad peruana (Prado Saldarriaga, 2023). Finalmente, un tercer problema es, a la vez, dogmático y práctico. Nos referimos a la noción de dinero en efectivo, que exige el tipo penal del delito regulado en el artículo 3° del Decreto Legislativo 1106. Al respecto, corresponde deslindar, expresamente, si un activo virtual o criptomoneda puede adquirir tal condición y naturaleza de dinero en efectivo.

A continuación, se ensayará en torno a los problemas planteados con algunas soluciones dogmáticas y prácticas.

4.1. Los activos virtuales son objeto del delito de lavado

Con relación al primer problema planteado, no cabe duda de que los activos virtuales o criptomonedas son también funcionalmente una forma distinta o innovada de activos o bienes. Como ya se ha señalado, son "representaciones digitales de valor que no son emitidas o garantizadas por un banco central o una autoridad pública, no están necesariamente vinculadas a una moneda legalmente establecida y no poseen un estado legal de moneda o dinero". Sin embargo, en el presente "son aceptadas por personas físicas o jurídicas como medio de intercambio y que pueden transferirse, almacenarse y comercializarse electrónicamente" (SBS,

2019a, p. 20). Es decir, constituyen también una manifestación de patrimonio o riqueza virtual, inmaterial e intangible. De esta manera, su naturaleza y función permiten que se les pueda identificar e interpretar también como objeto de acción de los delitos de lavado de activos que regula el Decreto Legislativo 1106. Es más, la nota interpretativa de la 15° recomendación del GAFI establece lo siguiente: "los países deben considerar a los activos virtuales como "bienes", "productos", "fondos", "fondos y otros activos" u otros activos de "valor equivalente". Los países deben aplicar las medidas pertinentes en virtud de las recomendaciones del GAFI a los activos virtuales" (GRAFILAT, 2018b, p. 77). Asimismo, en el literal i del artículo 2 del texto de Convención de las Naciones Unidas contra la ciberdelincuencia, aprobado en Nueva York el 9 de agosto de 2024 , los activos virtuales son considerados expresamente como bienes que pueden ser objeto de operaciones de lavado del producto del delito en los términos que regula también el artículo 17 de dicho documento: " i) Por bienes se entenderá los activos de cualquier tipo, corporales o incorporales, muebles o inmuebles, tangibles o intangibles, incluidos los activos virtuales, y los documentos o instrumentos legales que acrediten la propiedad u otros derechos sobre dichos activos."

Lo expuesto resulta suficiente para admitir, desvalorar y sancionar penalmente como delitos de lavado todas las operaciones o transacciones que impliquen la conversión, transferencia, adquisición o el ocultamiento y tenencia de activos virtuales de origen ilegal. Por consiguiente, aceptar tal posibilidad operativa y de uso criminal de los activos virtuales compatibiliza plenamente con una interpretación funcional sobre el objeto de acción del delito en los tipos penales contenidos en los artículos 1° y 2° del Decreto Legislativo 1106.

4.2. Los actos de lavado de activos virtuales son típicos y punibles

En lo que concierne al segundo de los problemas dogmáticos planteados, tampoco concurren mayores dificultades para la subsunción típica de las modalidades frecuentes de lavado de activos virtuales en los tipos penales de los artículos 1° y 2° del Decreto Legislativo 1106. Efectivamente, todas las tipologías hasta ahora conocidas de lavado de activos virtuales pueden asimilarse plenamente a las conductas tipificadas en aquellos artículos. Es decir, se manifiestan mayormente como modalidades delictivas y punibles de adquirir, transformar, permutar, transferir o mezclar activos virtuales de origen ilícito. Además, el que todas estas operaciones o transacciones con activos virtuales se ejecuten en o desde el ciberespacio para ocultar o evitar la detección o el decomiso de ganancias ilícitas del crimen organizado, no impiden que ellas produzcan impactos económicos y criminógenos nocivos en el mundo real (Valdés Trapote, 2022). En consecuencia, todas esas conductas también constituyen formas de conversión, transferencia,

ocultamiento o tenencia de activos de origen ilegal como las que describen y sancionan los mencionados artículos 1° y 2° del Decreto Legislativo 1106.

De acuerdo con lo señalado anteriormente, solo se requiere que los operadores del sistema penal adopten una interpretación funcional y normativa sobre dicho modus operandi, así como sobre su conexión o eficacia final para la legitimación aparente o el aseguramiento de los productos ilegales del crimen organizado.

4.3. Los activos virtuales no son dinero en efectivo

Sin embargo, respecto al tercer problema planteado, no se ve posibilidad de asimilación hermenéutica de un lavado de activo a la condición de dinero en efectivo. Por tanto, en torno a ello se requiere necesariamente de una reforma legislativa. Fundamentalmente, en el artículo 3 el Decreto Legislativo 1106 la disposición legal tipifica y sanciona expresamente el delito de transporte, traslado, ingreso o egreso del territorio nacional de dinero en efectivo o de instrumentos financieros negociables al portador. Esto es, la norma legal citada es expresa e inequívoca para identificar al objeto de acción del hecho punible. Efectivamente, el tipo penal considera específicamente que tienen esa condición únicamente el "dinero en efectivo" y los "instrumentos financieros negociables al portador". Es más, cabe recordar que este delito fue incorporado en el Decreto Legislativo 1106 para dar cumplimiento a lo dispuesto en la Recomendación 32 del GAFI sobre "Transporte en efectivo", la cual, de manera taxativa, refiere lo siguiente:

> Los países deben contar con medidas establecidas **para detectar el transporte físico transfronterizo de moneda e instrumentos negociables**, incluyendo a través de un sistema de declaración y/o revelación.
> Los países deben asegurar que sus autoridades competentes cuenten con la autoridad legal **para detener o restringir moneda o instrumentos negociables al portador** sobre los que se sospecha una relación con el financiamiento del terrorismo, el lavado de activos o delitos determinantes, o que son declarados o revelados falsamente.

Además, en el glosario de términos de la aludida nota interpretativa del GAFI, se consigna que el término transporte físico transfronterizo "se refiere al transporte físico entrante o saliente de moneda o instrumentos negociables al portador desde un país hacia otro país". Pero también se precisa que ello comprende tres modalidades de transporte: "(1) transporte físico por una persona natural o en el equipaje o vehículo que acompaña a esa persona; (2) cargamento de moneda o INP mediante carga en contenedores, o (3) el envío por correo de moneda o INP por una persona natural o una persona jurídica". En consecuencia, no queda duda

de que el delito tipificado en el artículo 3 del Decreto Legislativo 1106 exige como objeto de acción siempre moneda fíat, esto es, un tipo de activos de naturaleza necesariamente física o material como el dinero de curso legal. Dicha calidad y condición no tiene ni puede tener un activo virtual por más que se le denomine moneda virtual o criptomoneda, sobre todo porque no cuenta con ese estatus ni posee el reconocimiento legal de dinero. Es más, esto último, en el caso peruano, ha sido ratificado públicamente y de manera reiterada por el Banco Central de Reserva del Perú (BCRP), aclarando en sus comunicados oficiales que "las denominadas criptomonedas o criptoactivos en general no constituyen moneda de curso legal y no cumplen plenamente las funciones de dinero como medio de cambio, unidad de cuenta y reserva de valor". Cabe agregar que, en el caso de las monedas digitales, son activos virtuales que cuentan con el respaldo de un Banco Central, como ocurre actualmente en El Salvador con el bitcoin. Sin embargo, no se cumple plenamente la exigencia típica del artículo 3 del Decreto Legislativo 1106, pues no son materialmente "dinero en efectivo" (Olcese, 2022, pp. 44-45.

De acuerdo con lo expuesto líneas arriba, cabe concluir que no es posible subsumir, por vía de interpretación en la tipicidad del artículo 3° del Decreto Legislativo 1106 (Prado Saldarriaga, 2023, pp. 121-152), el ingreso o salida del territorio nacional de una billetera digital con criptomonedas de origen ilícito. Fundamentalmente, no se trata del transporte, ingreso o salida de dinero de curso legal ni tampoco de dinero en efectivo. Por tanto, cualquier intento o planteamiento hermenéutico en sentido contrario resultará ser una analogía negativa y contraria al principio de legalidad. Además, las criptomonedas tampoco cuentan, de momento, con el reconocimiento o respaldo formal que posee cualquier tipo de instrumento financiero negociable "al portador". En términos concretos y prácticos, los actos de transporte, traslado, ingreso o egreso del territorio nacional de activos virtuales de origen ilícito almacenados en cualquier clase de soporte informático o digital (billeteras digitales, computadoras, *laptop, tablets*, teléfonos celulares e incluso en un USB) es todavía para la legislación penal peruana una conducta atípica y carente de relevancia penal. Ello no sólo constituye una sensible vulnerabilidad, sino que constituye también un alto riesgo de prácticas de lavado de las ganancias ilegales del crimen organizado. En lo esencial, como se ha explicado anteriormente, quien traslade o porte consigo monedas virtuales podrá luego negociar plenamente con ellas o convertirlas en dinero en efectivo o intercambiarlas por otras monedas virtuales de procedencia lícita o ilícita.

Resulta entonces oportuno plantear de *lege ferenda* una urgente y prioritaria reformulación del texto actual del aludido artículo 3°. En efecto, se requiere construir una redacción legal más innovadora e ingeniosa, por lo que, al incorporar un texto normativo, es necesario considerar también sus alcances a las

monedas virtuales. Es decir, se debe añadir en el texto legal vigente del artículo 3° una referencia enunciativa más refinada e inclusiva de los "activos virtuales" o "monedas virtuales" o incorporar a los activos virtuales como un tipo de bienes, efectos o ganancias también en el artículo 10° del Decreto Legislativo 1106.

4.4. Configuración de delitos periféricos con activos virtuales

Finalmente, para concluir el examen realizado, el delito de lavado de activos virtuales y sobre la utilidad de los tipos penales contenidos en el Decreto Legislativo 1106 para reprimir tales actos, es importante referirse a los delitos periféricos regulados en los artículos 5° y 6°. Esto es, a los delitos de omisión de reporte de operaciones o transacciones sospechosas y de rehusamiento, retardo o falsedad de información. En torno a tales hechos punibles es de mencionar que no se detecta ninguna limitación de legalidad típica para su configuración y punibilidad en relación con conductas que involucren activos virtuales. Especialmente, los delitos periféricos no son actos de lavado de activos virtuales sino solamente incumplimientos de obligaciones legales o de mandatos dispuestos por autoridad competente; son delitos típicos de mera desobediencia. Por ello, para que los delitos de los artículos 5° y 6° puedan producirse con referencia a activos virtuales radica solo en la existencia de esas obligaciones de reporte de operaciones sospechosas detectadas o, también, de los requerimientos oficiales y determinados de información que formule una autoridad competente. Ahora bien, cabe destacar que desde finales de julio de 2023 el Decreto Supremo N°006-2023-JUS incorporó formalmente como sujeto obligado a informar operaciones y transacciones sospechosas a los proveedores de servicios con activos virtuales-PSVA. Por tanto, ellos pueden ahora incurrir en las modalidades dolosas o culposas del delito de omisión de reporte que tipifica y sanciona el artículo 5° del Decreto Legislativo 1106. Es más, recientemente se ha publicado en el diario oficial El Peruano una separata especial que reúne las normas para la prevención del lavado de activos y del financiamiento del terrorismo aplicable a los proveedores de servicios de activos virtuales-PSAV bajo supervisión de la Unidad de Inteligencia Financiera del Perú. Se trata de la Resolución SBS N.º 02648-2024 del 30 de julio de 2024. Es un documento amplio y detallado que reúne sistemáticamente disposiciones que definen conceptos operativos sobre activos virtuales. Además, identifica las transacciones que se realizan con intervención de los PSAV y a favor de terceros. Incluye también un pormenorizado marco regulador relacionado con la denominada "regla del viaje", así como con el umbral de las operaciones reportables y que se ha fijado en 1000 dólares americanos o su equivalente en moneda nacional. En ese mismo sentido, también definen con claridad la oportunidad, identificación y reporte de operaciones o transacciones inusuales y sospechosas. Se norma, igualmente, lo concerniente al perfil y

funciones que deberá cumplir el Agente de Cumplimiento de los Proveedores de Servicios de Activos Virtuales. En torno a ellos se resalta la obligación de la debida diligencia en la identificación de las operaciones y detección de aquellas inusuales o sospechosas. Asimismo, esta obligación hace expresa referencia a los deberes de confidencialidad de los reportes y sus correspondientes exenciones de responsabilidades civiles o penales en favor del reportante. Por último, se alude a las buenas prácticas en la aplicación de los programas de cumplimiento como identificar el mapa de riesgos y la configuración de normatividad interna ética, así como el desarrollo de acciones de capacitación que se deben brindar al personal adscrito al Proveedor de Servicios de Activos Virtuales-PSAV.

Finalmente, cabe destacar los plazos para la vigencia de este inédito sistema normativo, así como de los regímenes transitorios sobre disposiciones especiales como las alusivas a la regla del viaje, lo cual es pertinente y justificado dado lo novedoso de toda esta normatividad en nuestro país. Por ejemplo, si bien el aludido sistema normativo entró en vigor al día siguiente de su publicación en el diario oficial El Peruano, se prevé otros plazos más extensos como los dos años para la "regla de viaje".

Ahora bien, como comentario final, cabe considerar lo oportuno y completo de la Resolución SBS N.º 02648-2024, porque nos alinea con las tendencias actuales que desarrolla la legislación internacional y comparada más avanzada. Corresponde, pues, augurar que las nuevas normas sean eficaces. Esto habrá de reflejarse en los próximos reportes de operaciones sospechosas de lavado de activos virtuales que haga la UIF del Perú, así como en las tipologías que este organismo vaya detectando.

En lo concerniente al delito de rehusamiento, retardo o falsedad de información, no hay necesidad de ninguna adición o reformulación que realizar en el texto vigente del artículo 6°. Lo relevante será, únicamente, que los requerimientos de información que se formulen (datos específicos de una operación o intervinientes en ella o documentación pertinente), por ejemplo, a un PSAV, deberán estar siempre vinculados a una investigación o proceso penal por delito de lavado de activos. Asimismo, a quien le sea requerida tal información se encuentra en la obligación legal de suministrarla en su integridad y oportunamente.

5. A MODO DE CONCLUSIÓN

Para finalizar este breve examen sobre los delitos de lavado de activos virtuales en la legislación peruana, cabe concluir que la normatividad vigente se encuentra en gran medida apta para ese propósito político criminal. Sin embargo, es necesario precisar que el articulado vigente del Decreto Legislativo 1106 puede perfilarse mejor para aquellos efectos con puntuales ajustes y modificaciones legales en sus

disposiciones penales y especialmente lo que atañe al objeto virtual de las acciones delictivas (criptomonedas). Paralelamente, se deben ampliar las disposiciones de naturaleza preventiva recogiendo las diferentes recomendaciones formuladas por el GAFI, así como las mejores experiencias legislativas desarrolladas en el derecho comparado. Al respecto, es de tener en cuenta que el lavado de activos virtuales ya es en el Perú una nueva tipología del crimen organizado y no solo una grave amenaza. En ese sentido es pertinente tener en cuenta lo señalado por Gómez Iniesta (2023):

Son muchos los desafíos legales que plantea el mundo digital, pero debemos estar a la altura de los retos que igualmente suscita el ciberblanqueo. La evolución permanente de las nuevas tecnologías ofrece la posibilidad de efectuar operaciones transfronterizas de realización rápida y con anonimato, relativo en algunos casos, total en otros, dificultando la eficacia de las normas (p. 1184).

REFERENCIAS

Aguedo, B. (19 de marzo de 2019). *Apuntes introductorios sobre el riesgo de lavado de activos y financiamiento del terrorismo en las transacciones con criptomonedas.* The Crypto Legal.https://thecryptolegal.com/apuntes-introductorios-sobre-el-riesgo-de-lavado-de-activos-y-financiamiento-del-terrorismo-en-las-transacciones-con-criptomonedas/.

Arango-Arango, C.A., Barrera-Rego, M.M., Bernal-Ramírez, J.F., y Boada-Ortiz. (2018).Criptoactivos. Banco de la República-Colombia. https://www.banrep.gov.co/es/publicaciones/documento-tecnico-criptoactivos.

Bodoque Agredano, A. y Orduna Lanau, A. (2022). *Guía de investigación en el lavado de activos mediante criptodivisas.* Disponible en: https://elpaccto.eu/wp-content/uploads/2022/07/Guia-Lavado-Activos-Criptodivisas.pdf

Cuadros, F. (2022). INEI: 10 millones de peruanos trabajan en la informalidad. Disponible en: https://larepublica.pe/economia/2022/11/20/inei-10-millones-de-peruanos-trabajan-en-la-informalidad-empleos-pandemia-covid-19-mef-china-armando-mendoza-farid-matuk-sunat

European Union Agency for Law Enforcement Cooperation (2023). IOCTA.

Financial Crime Academy (2024). *Lavado de dinero en la era digital: explorando el papel de los activos virtuales.*

Financial Action Task Force. (2020). *Money Laundering and Terrorist Financing Red Flag Indicators Associated with Virtual Assets.* The Financial Action Task Force and Organisation for Economic Co-operation and Development.

Financial Action Task Force. (2022). *Targeted Update on Implementation of the FATF Standards on Virtual Assets Service Providers.*

Guardia Quispe, K. (13 de marzo de 2023). UIF: Empresas que ofrecen criptomonedas cerca de ser reguladas tras luz verde del Minjus. *Diario Gestión.* https://gestion.pe/economia/empresas/uif-sbs-peru-fiscalua-lavado-de-activos-criptomonedas-criptoactivos-minjus-uif-empresas-que-ofrecen-criptomonedas-cerca-de-ser-reguladas-tras-luz-verde-del-minjus-noticia/

Gómez Iniesta, D. J. (2023). Utilización de las Nuevas Tecnologías en la Comisión del Blanqueo de Dinero. En E. O. Álvarez Yrala (Coord.). *Derecho penal y Dignidad Humana. Libro Homenaje al Profesor Felipe Villavicencio Terreros* (Vol. 2, pp. 1151-1190). Grijley.

Grupo de Acción Financiera Internacional. (2015). *Directrices para un enfoque basado en riesgos. Monedas Virtuales.*

Grupo de Acción Financiera Internacional. (2021). *Guía actualizada para un enfoque basado en el riesgo. Activos virtuales y proveedores de servicios de activos virtuales.*

Grupo de Acción Financiera de Latinoamérica. (2021). Informe Tipologías Regionales de LA/FT 2019-2020. https://www.smv.gob.pe/ConsultasP8/temp/Informe%20de%20Tipolog%c3%adas%20Regionales%20de%20LA-FT%202019-2020%20%20GAFILAT%20%202021.pdf

Grupo de Acción Financiera de Latinoamérica. (2018a). *Ejercicio Bienal de Tipologías Regionales. Casos y Tipologías Regionales 2017-2018.* Grupo de Acción Financiera de Latinoamérica y Unidad de Análisis Financiero y Económico.https://www.gafilat.org/index.php/es/biblioteca-virtual/gafilat/documentos-de-interes-17/tipologias-17/3126-informe-tipologias-regionales-gafilat-2018/file

Grupo de Acción Financiera de Latinoamérica. (2018b). *Las Recomendaciones del GAFI. Estándares Internacionales sobre la Lucha contra el Lavado de Activos, el Financiamiento del Terrorismo y de la Proliferación de Armas de Destrucción Masiva.* Organización para la Cooperación y el Desarrollo Económicos y Grupo de Acción Financiera de Latinoamérica.

Notes de Seguretat. (12 de abril de 2023). Las fuerzas policiales ante las criptomonedas y el 'blockchain'. *Generalitat de Catalunya*. https://notesdeseguretat.blog.gencat.cat/2023/04/12/las-fuerzas-policiales-ante-las-criptomonedas-y-el-blockchain/

Olcese, B. (2022). *Criptonegocios: el sistema que cambió las reglas de juego.* Nóstica editorial.

Observatorio Nacional de Política Criminal (2021). El tráfico de vida silvestre en la Amazonía. Ministerio de Justicia de Derechos Humanos. Disponible en: https://cdn.www.gob.pe/uploads/document/file/2517362/El%20tr%C3%A1fico%20de%20vida%20silvestre%20en%20la%20Amazon%C3%ADa.pdf.pdf?v=1637960089

Observatorio Nacional de Política Criminal (2022). La Tala Ilegal en la Amazonía Peruana. Ministerio de Justicia de Derechos Humanos. Disponible en: https://cdn.www.gob.pe/uploads/document/file/3095185/Documento%20-%20La%20tala%20ilegal%20en%20la%20Amazon%C3%ADa%20peruana.pdf.pdf?v=1654203896

Pérez López, X. (2017). Las Criptomonedas: consideraciones generales y empleo de las criptomonedas como instrumento de blanqueo de capitales en la Unión Europea y en España. *Revista de Derecho Penal y Criminología*, (18). https://revistas.uned.es/index.php/RDPC/article/view/24454.

Prado Saldarriaga, V. R. (1997). El lavado de dinero como delito internacional. *Política Internacional*, (47), 129-136.

Prado Saldarriaga, V.R. (2019). *Lavado de Activos y Organizaciones Criminales en el Perú*. IDEMSA.

Prado Saldarriaga, V.R. (2023). Lavado de Activos virtuales. Nueva tipología del crimen organizado en el Perú. Gaceta Jurídica.

Santiago Gonzáles, J. (20 de mayo de 2021). *Riesgo de Lavado. Auge de las Criptomonedas.* Iberoamericana. Educación Ejecutiva. https://www.ibee.education/blog-articulo/riesgo-de-lavado-de-dinero-el-auge-de-las-criptomonedas/

Superintendencia de Banca, Seguros y AFP (SBS). (2019a). *Activos Virtuales y Proveedores de Activos Virtuales: Diagnóstico Situacional. Legislación Comparada y Exposición a los Riesgos de LA/FT en el Perú*.https://www.sbs.gob.pe/portals/5/jer/estudio-analisis-riesgo/estudio%20activos%20virtuales%20y%20psav.pdf

Superintendencia de Banca, Seguros y AFP (SBS). (2019b). Prevención del lavado de activos y financiamiento del terrorismo. *Boletín Informativo, 78.* https://www.sbs.gob.pe/portals/5/jer/boletin-informativos/2019/boletin_informativo_78.pdf