BAJO LA LUPA:

¿QUÉ TAN CIERTO ES QUE LAS CRIPTOMONEDAS SON PROPICIAS PARA EL LAVADO DE ACTIVOS?

Autores:
Adolfo Morán Cavero
Beatriz Alexandra Aguedo Huiza
Karen Vanessa Dávila Neyra

Bajo la lupa: ¿Qué tan cierto es que las criptomonedas son propicias para el lavado de activos?

ADOLFO MORÁN CAVERO[1]
BEATRIZ ALEXANDRA AGUEDO HUIZA[2]
KAREN VANESSA DÁVILA NEYRA[3]

SUMARIO

I. INTRODUCCIÓN.

El 2008 fue un año de varios acontecimientos importantes. Dos valen la pena recordar: la quiebra de Lehman Brothers y la publicación del *whitepaper* de Bitcoin. Mientras el sistema financiero mundial entraba a una de sus peores crisis, salía a la luz un nuevo sistema de transferencias de valor y pagos digitales.

[1] Bachiller en Derecho por la Pontificia Universidad Católica del Perú (PUCP). Co-fundador y Director Ejecutivo de la Asociación Lawgic Tec. Ha sido Editor General del blog The Crypto Legal. Actualmente, se desempeña como Consultor Legal en el área de Regulación Financiera & FinTech de EY Law (Ernst & Young). Especialista en temas de Regulación Financiera, FinTech, Blockchain y Criptomonedas.

[2] Bachiller en Derecho por la Pontificia Universidad Católica del Perú (PUCP). Candidata a magíster en Derecho Civil y Comercial por la Universidad Xi'An Jiaotong. Especialista certificada en Prevención de Lavado de Activos (ACAMS). Coordinadora del Círculo de Estudios Chinos sección Derecho del Instituto Confucio PUCP, miembro del Grupo de Investigación en Derecho Bancario y Financiero de la PUCP y Asociada de Lawgic Tec. Actualmente está especializándose en temas de Compliance, Gestión de Riesgos y Prevención del Lavado de Activos y Financiamiento del Terrorismo.

[3] Abogada por la Pontificia Universidad Católica del Perú se encuentra cursando la maestría en Política y Gestión Tributaria con mención en Auditoria Tributaria de la Facultad de Contabilidad en la Universidad Mayor de San Marcos. Asimismo, es directora de la Comisión de Relaciones Públicas y Marketing de la Asociación Lawgic Tec.

El creador de Bitcoin es –el todavía desconocido– Satoshi Nakamoto. Detrás del seudónimo, una persona o grupo de personas buscaron una alternativa al sistema financiero tradicional que fue duramente cuestionado en los años venideros. [4]

Bitcoin se ha abierto camino como una alternativa realmente viable, en donde no intervienen bancos ni otras entidades financieras. Tal ha sido el éxito de Bitcoin, que fue inspiración para que en los años que siguieron se fueran lanzando muchos más proyectos del mismo tipo (Ethereum, Litecoin, Dash, etc.). El factor común entre todos estos es que hacen uso de criptomonedas.[5]

Las criptomonedas o criptoactivos son las monedas o unidades de cambio en estos sistemas descentralizados. Cada uno hace uso de su propia criptomoneda para diversos fines.[6] Asimismo, tienen un valor cotizable en dólares estadounidenses y son conocidas por su volatilidad.

Efectivamente, entre los años 2010 y 2017, muchos inversionistas profesionales y no profesionales[7] hicieron grandes sumas de dinero gracias a las criptomonedas. La estrategia era simple: comprar mucho y barato para luego venderlos cuando su valor aumente considerablemente.[8] Esta simple estrategia volvió a muchos en millonarios de "la noche a la mañana". [9]

Sin embargo, las criptomonedas como los bitcoins no solo sirven para especular y generar ganancias, sino que sirven también para transferir fondos de un lugar a otro, sea a escala nacional o internacional. Lo mejor de todo, no necesitas identificarte ni pasar por el sistema financiero para efectuar dicha transferencia. Todo ocurre en el mundo virtual.

El anonimato (o seudonimato) y la falta de supervisión de estas redes de transferencias y pagos ha significado que se asocie –casi naturalmente– el uso de criptomonedas a actividades ilícitas, como el lavado de activos y el financiamiento del terrorismo (LA/FT). Tanto es así, que el Grupo de Acción Financiera Internacional (GAFI), que es la institución internacional que vela por la prevención del LA/FT a nivel mundial, ha instado a que los gobiernos elaboren políticas y normas que tengan por finalidad regular las operaciones con criptomonedas[10].

En Perú, a la fecha de presentación de este artículo, todavía no se ha publicado una ley o reglamento que exija a las empresas que operan con criptomonedas (ej. las bolsas de criptomonedas) a que adopten mecanismos para la prevención del LA/FT. Tampoco existen

[4] Movimientos como Occupy Wall Street cuestionaban las acciones adoptadas por el gobierno de los Estados Unidos frente a la crisis y ponían sobre la mesa las desigualdades sociales; por ejemplo, los privilegios de las grandes empresas.
[5] También hay otros factores comunes, como el uso de una blockchain o cadena de bloques.
[6] Por ejemplo, en Ethereum, la criptomoneda ether es también usada como "combustible" o "gas" para ejecutar aplicaciones construidas en esta plataforma.
[7] Con inversionista no profesional nos referimos a aquellos que invierten dinero en un activo o instrumento financiero sin una clara estrategia de inversión, sin mayor educación en finanzas o que se basan principalmente en recomendaciones de amigos y familiares para tomar sus decisiones de inversiones; también conocidos como *sheep* (ovejas) en la jerga financiera en inglés.
[8] Para mayor información sobre este boom de las criptomonedas y la psicología del inversionista de criptomonedas, véase García Long, Sergio y Adolfo Morán Cavero (2019). *Criptomonedas y Psicología Financiera.* En: Chipana, Jhoel (Coord.), Derecho y Nuevas Tecnologías: El impacto de una nueva era, pp. 243-262.
[9] Por ejemplo, a inicios de febrero del 2017, un bitcoin costaba alrededor de 1,000 dólares estadounidenses. Si una persona compraba 50 bitcoins a ese precio, para el 17 de diciembre del mismo año sus bitcoins valdrían en total 1 millón de dólares estadounidenses aproximadamente.
[10] Por ejemplo, en Argentina existe ya legislación que obliga a los sujetos obligados de dicho país a tomar medidas reforzadas cuando un cliente efectúa transacciones con criptomonedas.

disposiciones específicas sobre las criptomonedas aplicables a las entidades financieras peruanas.[11]

Sin embargo, la falta de regulación especial no es motivo para que los sujetos obligados[12] a reportar a la Unidad de Inteligencia Financiera (UIF) no consideren a las criptomonedas dentro de su gestión de riesgos de LA/FT en caso de presentarse una operación o cliente vinculado a estos activos virtuales.

En este contexto, en el presente artículo se realizará un análisis de los vínculos de las criptomonedas con el delito de lavado de activos, se abordarán las directrices y recomendaciones elaboradas por el GAFI, se explicarán las respuestas de los sujetos obligados –especialmente bancos– a las operaciones con criptomonedas frente al riesgo de LA/FT y, finalmente, se presentarán nuestras conclusiones.

II.¿POR QUÉ SE ASOCIA A LAS CRIPTOMONEDAS CON EL LAVADO DE ACTIVOS?

Las criptomonedas llevan en su nombre la alusión a la criptografía. ¿Qué es esto? La criptografía hace referencia a aquellas técnicas o métodos utilizados para cifrar o codificar un mensaje, de modo que este se vuelva ininteligible para las personas no autorizadas a conocer su contenido. En otras palabras, las técnicas criptográficas se utilizan para asegurar la confidencialidad de un mensaje.

El uso de técnicas criptográficas a lo largo de la historia no ha sido poco común. De hecho, el uso de técnicas para mantener un mensaje confidencial se remonta hasta épocas anteriores al inicio de la era cristiana. Por ejemplo, Julio César, el famoso militar y político romano, utilizó una técnica de cifrado que consistía en cambiar las letras de palabras por otras que les seguían, de modo que en lugar de colocar una "A" ponía una "D", y así sucesivamente con todas las demás[13]. De esta manera, el que no conocía de esta técnica, no podía descifrar el mensaje.

Ahora bien, ¿cómo se utiliza la criptografía en las criptomonedas?[14] De dos maneras. La primera consiste en utilizar criptografía de clave asimétrica para efectuar una transacción con criptomonedas. La segunda para la creación de bloques compuestos de varias transacciones que son unidos en la cadena de bloques o *blockchain*.

En el primer caso, un usuario que tiene en su poder bitcoins debe hacer uso de la combinación de una llave pública y una llave privada para enviar o transferir bitcoins a otro usuario. Todos los usuarios tienen una dirección pública[15] que pueden compartir a otros usuarios para que les transfieran bitcoins[16]. De esta manera, para transferir los bitcoins, el titular de estas criptomonedas debe utilizar su llave privada[17] para "firmar digitalmente" la transacción, de modo que el sistema[18]

[11] Sin embargo, es de conocimiento público que la regulación sobre este tema está en camino. A inicios del año 2020, la jefa del departamento de Supervisión de Riesgo Operacional de la Superintendencia de Banca, Seguros y AFP (SBS) indicó que esta entidad se encontraba preparando el reglamento correspondiente.
[12] Son aquellas personas naturales y personas jurídicas que se dedican a las actividades previstas en el artículo 3 de la Ley N° 29038.
[13] Para cifrar sus mensajes, Julio César desplazaba las letras tres espacios en el alfabeto. Por ejemplo, si el mensaje es HOLA, mediante esta técnica de cifrado, el mensaje codificado sería KROD.
[14] Utilizaremos Bitcoin como ejemplo, no todas las criptomonedas funcionan de la misma manera.
[15] La dirección pública es una serie de números y letras derivado de la llave pública.
[16] Funciona como un número de cuenta bancaria.
[17] Es también una serie de números y letras que solo el titular debe conocer. También sería análogo a una clave secreta.
[18] Esta verificación lo hacen los nodos de la red de Bitcoin.

podrá asociar su llave pública (dirección pública) con su llave privada y verificar que es el autorizado para gastar los bitcoins registrados en *blockchain* (Antonopoulos, 2017, p. 57).

En el segundo caso, los mineros en Bitcoin utilizan criptografía para producir bloques válidos con transacciones que serán integrados en la *blockchain*[19]. Para ello, se debe efectuar una función hash criptográfica. En términos más simples, se trata de la aplicación de un algoritmo *hash* que convierte cualquier clase de información a una serie de longitud determinada de números y letras. Esta serie de caracteres es única y sirve para identificar el bloque con transacciones, haciéndola también única con respecto a otras. De esta manera, se forma una cadena de bloques unidos correlativamente por hashes o identificadores únicos (Antonopoulos, 2017, pp. 228 y ss.). [20]

Como se aprecia, la criptografía está enteramente incluida en Bitcoin y en otros sistemas. Es un elemento esencial. Sin embargo, para los fines de este artículo importa sobre todo la criptografía de clave asimétrica que hemos explicado, ya que es este método criptográfico, junto con todo el sistema, que permite realizar transacciones seguras sin necesidad de revelar datos personales. Solo se necesita del par de llaves (pública y privada).

De este modo, un usuario de Bitcoin se identifica frente a otros pares únicamente utilizando su dirección pública, que es también una serie de números y letras. Con solo ver la dirección pública no es posible saber a quién le pertenece, es necesario contar con mayor información. Por ello, se dice comúnmente que Bitcoin es un sistema anónimo o seudónimo, ya que permite la interacción entre usuarios sin revelar sus identidades.

A primera vista, esta característica de Bitcoin y de otras redes que utilizan criptomonedas resultaría atractiva para personas que buscan realizar operaciones financieras sin revelar sus identidades ni sus propósitos, y, sobre todo, para no dejar rastros, lo cual lo hace idóneo para el lavado de activos.

2.1. ¿En qué consiste el lavado de activos?

¿Qué es el lavado de activos? Se trata de un delito complejo que tiene por finalidad ocultar mediante distintas actividades los fondos o activos obtenidos de una fuente ilícita.[21] De esta manera, se da apariencia de origen lícito a dinero que ha sido conseguido a través de actividades delictivas.

Por ejemplo, el dinero obtenido por un delincuente, de una persona a la que ha extorsionado, que luego es ingresado al sistema financiero con el fin de confundir el origen ilícito. En el entorno virtual, las actividades ilícitas estarían relacionadas a ransomware[22] y estafas mediante phishing[23], entre otras actividades delictivas.

[19] Lo que busca un minero con este proceso es encontrar un valor *hash* dentro de un umbral determinado que permitirá validar el bloque candidato que creó anteriormente y de esta manera el bloque sea aceptado por todos los nodos como parte integrante de la cadena de bloques.
[20] Cabe señalar que los bloques son correlativos porque un bloque contiene también información del bloque anterior. En otras palabras, la identidad de un bloque depende en cierta medida de la información del bloque anterior.
[21] En el Perú, el delito de lavado de activos se encuentra tipificado en sus distintas modalidades en los artículos 1,2,3 y 4 del Decreto Legislativo N° 1106, Decreto Legislativo de lucha eficaz contra el lavado de activos y otros delitos relacionados a la minería ilegal y crimen organizado.
[22] El ransomware es un software malicioso que permite al atacante controlar la información almacenada, encriptándola y bloqueándola. Para desbloquear esta información, piden rescates que suelen ser pagadas con criptomonedas.
[23] El phishing es una técnica que consiste en enviar, normalmente, correos electrónicos masivamente, haciéndose pasar por entidades o personas fiables (ej. bancos, SUNAT, etc.). Estos correos electrónicos contienen enlaces que llevan a sitios web que tienen por finalidad extraer datos bancarios, entre otros.

El delito de lavado de activos normalmente está compuesto de 3 etapas. La primera etapa es la colocación y, consiste en ingresar los fondos de origen ilícito al sistema financiero[24]. La segunda etapa, conocida como conversión, consiste en diversificar el dinero de origen ilícito a través de diferentes operaciones (ej. inversiones, transferencias, etc.); lo que se busca es eliminar el rastro del origen ilícito. Finalmente, la tercera y última etapa es la integración e, implica que los fondos de origen ilícito se han mezclado completamente con activos de origen lícito mediante actividades económicas legales y cotidianas; esto hace casi imposible identificar y separar los fondos o activos de origen ilícito de los que no lo son (Villavicencio, 2011, pp. 5-6).

Durante mucho tiempo (y hasta ahora) el dinero en efectivo ha sido el medio de pago preferido y más utilizado por los lavadores para perpetrar este delito. La razón es obvia, el dinero en efectivo (i) permite fácilmente esconder el origen o la fuente, (ii) es fácil de mantener el control sobre los billetes[25] y (iii) existe la posibilidad de fragmentar fácilmente los montos obtenidos (Europol, 2015, p. 9).

Sin embargo, en los últimos años las criptomonedas han sido puestas bajo los reflectores.[26] Sucede que las criptomonedas y el dinero en efectivo comparten la característica de ser medios de pago que no necesitan de la revelación de la identidad de los usuarios, a diferencia de, por ejemplo, las tarjetas de crédito o débito.

Esto último facilita en gran medida esconder el origen de la fuente ilícita[27], aunque cabe decir que, a diferencia del *cash*, las transacciones con criptomonedas quedan registradas en una base de datos pública (*blockchain*), lo que constituye una importante herramienta para perseguir el delito de lavado de activos con criptomonedas.

Además, es importante considerar que una ventaja diferencial en el caso de las criptomonedas es que permiten realizar transferencias de fondos internacionalmente sin mayor trámite y de manera muy rápida (ej. en Bitcoin, aproximadamente entre 10 a 60 minutos).[28] Esto resulta ser una ventaja que antes no existía con los sistemas tradicionales de transferencia electrónica de fondos, que siempre implicaba la intervención de una entidad financiera o de una entidad complementaria o auxiliar.

Ahora bien, según las estadísticas de CipherTrace, en los primeros cinco meses del 2020 se han registrado crímenes con criptomonedas por un valor total de 1.36 mil millones de dólares estadounidenses. Sin embargo, de acuerdo con el reporte "The 2020 State of Crypto Crime" de Chainalysis, las transacciones relacionadas a crímenes (incluido el lavado de activos) representarían el 1.1% de todas las transacciones con criptomonedas[29].

[24] Esta etapa suele ser la más difícil de realizar y la que conlleva mayor riesgo para el delincuente.
[25] Quien lo tiene en su poder, lo controla.
[26] Principalmente, el uso de criptomonedas dentro de las etapas de lavado de activos estaría vinculado a los delitos informáticos. Es decir, un lavador utilizaría criptomonedas si es que el delito precedente es cometido en el ciberespacio; por ejemplo, mediante el pedido de un rescate con bitcoins (ransomware).
[27] De acuerdo con lo que señalamos anteriormente, si bien el registro de transacciones es público, lo único que una persona cualquiera podría verificar es que una dirección transfiere bitcoins a otra dirección; no pudiendo conocer a simple vista quién está detrás de esa dirección. Sin embargo, cabe anotar que, a pesar del uso de seudónimos en la red de Bitcoin (el caso paradigmático), sí ha sido posible anteriormente llegar a identificar a la persona detrás de una transacción ilícita con bitcoins. Por ejemplo, un caso resaltante es el de Ross Ulbricht, quien actualmente se encuentra encarcelado en los Estados Unidos, debido a que creó un *marketplace* de venta de drogas, y otros productos y servicios ilegales. Además de haber utilizado la red anónima Tor, dicho *marketplace* aceptaba bitcoins como medio de pago. Sin embargo, a pesar de toda esta privacidad, la FBI pudo dar con el paradero de Ulbricht.
[28] De acuerdo con el reporte "Cryptocurrency, Crime and Anti-Money Laundering" de junio de 2020 de CipherTrace, el 74% de transacciones con bitcoins entre bolsas de criptoactivos (*exchanges*) fueron transfronterizas.
[29] Data obtenida hasta el año 2019.

Teniendo en cuenta estas cifras, el uso de criptomonedas para lavar activos podría impulsarse considerablemente si es que comienzan a aparecer mayores tiendas online que acepten criptomonedas como medio de pago. De esta forma, será más fácil diversificar las criptomonedas de origen ilícito por medios virtuales, en lugar de estar convirtiendo estas criptomonedas en dinero en efectivo para confundirlas dentro de la economía formal (Europol, 2015, pp. 42-43).

Por ello, los sujetos obligados a reportar a la UIF deben conocer los riesgos de operar con criptomonedas, las cuales son parte de un fenómeno cada vez más cotidiano, y no rechazarlas por el simple desconocimiento. Vale la pena mencionar que, como se verá en las siguientes líneas, el GAFI ha elaborado directrices aplicables a operaciones con criptomonedas o criptoactivos, que son un importante punto de partida para la inclusión de estos activos virtuales en la economía formal y para enfrentar el lavado de activos.

III. GAFI Y LA PREVENCIÓN DEL LAVADO DE ACTIVOS.

El Grupo de Acción Financiera Internacional (GAFI) fue creado en 1989 como un organismo intergubernamental con el objetivo de establecer normas y promover la efectiva implementación de medidas de tipo legal y reglamentario, así como para la toma de acciones para combatir el lavado de activos, el financiamiento del terrorismo y otras amenazas a la integridad del sistema financiero.

A la fecha, el GAFI está conformado por 39 miembros y 9 grupos regionales como organismos asociados, entre ellos se encuentra el Grupo de Acción Financiera para América Latina (GAFILAT).

El GAFILAT fue creado en el 2000[30], el grupo constitutivo de representantes en América Latina estuvo conformado por los siguientes países: Argentina, Bolivia, Brasil, Chile, Colombia, Ecuador, Paraguay, Uruguay y Perú.

Ahora bien, el GAFILAT como organización intergubernamental tiene como fin prevenir y combatir el lavado de activos, financiamiento del terrorismo y el financiamiento de la proliferación de armas de destrucción masiva, por medio de la mejora continua de las políticas nacionales y la profundización de mecanismos de cooperación entre los países miembros.

Al respecto, debemos resaltar que el GAFILAT fue creado a semejanza del GAFI, adhiriéndose a las 40 Recomendaciones del GAFI como estándar internacional más reconocido contra el LA/FT, previendo el desarrollo de recomendaciones propias de mejora de las políticas nacionales para la lucha contra los delitos de LA/FT.

3.1. ¿Cuáles son las Recomendaciones del GAFI?

Las Recomendaciones del GAFI constituyen un esquema de medidas que los países deberían implementar para combatir el lavado de activos, el financiamiento del terrorismo, y el financiamiento de la proliferación de armas de destrucción masiva.

Debemos precisar que en vista que los países tienen distintas regulaciones y distintos sistemas financieros, las Recomendaciones del GAFI proponen un estándar internacional para que los países puedan implementar las medidas a sus circunstancias particulares, el cual comprende esencialmente los siguientes puntos (FAFT, 2019a):

[30] Cabe precisar que, en ese entonces, se denominaba Grupo de Acción Financiera de Sudamérica (GAFISUD), pero con la incorporación de países del Caribe se aprobó el cambio de su denominación a GAFILAT.

- Identificar riesgos y desarrollar políticas y coordinación local;
- Luchar contra el lavado de activos, financiamiento del terrorismo y financiamiento de la proliferación de armas de destrucción masiva;
- Aplicar medidas preventivas para el sector financiero y otros sectores;
- Establecer poderes y responsabilidades de las autoridades competentes (por ejemplo: autoridades investigativas, de orden público y de supervisión) y otras medidas institucionales;
- Mejorar la transparencia y la disponibilidad de la información de titularidad de beneficio de las personas y estructuras jurídicas; y
- Facilitar la cooperación internacional.

Algunas de estas 40 Recomendaciones que vale la pena destacar de manera resumida para este artículo son las siguientes (FAFT, 2019a):

Recomendación 1 vinculada a la "Evaluación de riesgos y aplicación de un enfoque basado en el riesgo" que aborda la identificación, evaluación, aplicación y entendimiento de los riesgos de lavado de activos y financiamiento del terrorismo, a fin de tomar medidas, bajo un enfoque basado en riesgos (EBR), para prevenir o mitigar el LA/FT de manera proporcional a los riesgos identificados.

En ese sentido, la primera Recomendación busca que los países, a través de sus entidades financieras y actividades y profesiones no financieras designadas (APNFD), identifiquen, evalúen y tomen acciones eficaces para mitigar los riesgos de LA/FT.

Recomendación 2 vinculada a la "Cooperación y coordinación nacional" mediante la cual se sugiere la necesidad de que los países tengan la certeza que, las autoridades que hacen las políticas, la Unidad de Inteligencia Financiera (UIF), las autoridades del orden público, los supervisores y otras autoridades competentes relevantes, a nivel de formulación de políticas y operativo, cuenten con mecanismos eficaces que les permita cooperar y, cuando corresponda, entablar una coordinación a nivel interno en el desarrollo e implementación de políticas y actividades para combatir el lavado de activos, el financiamiento del terrorismo y el financiamiento de la proliferación de armas de destrucción masiva.

Recomendación 3 vinculada a "Delito de lavado de activos" que establece el deber de tipificar el lavado de activos conforme a la Convención de Viena y la Convención de Palermo. Asimismo, se precisa que los países deberán aplicar el delito de lavado de activos a todos los delitos graves, con la finalidad de incluir la mayor cantidad posible de delitos relevantes.

Recomendación 15 vinculado a "Nuevas tecnologías"; al respecto el GAFI precisa que tanto los países como las entidades financieras deberán identificar y evaluar los riesgos de lavado de activos y/o financiamiento del terrorismo que pudieran surgir con respecto a:

(a) el desarrollo de nuevos productos y nuevas prácticas comerciales, incluyendo nuevos mecanismos de envío, y

(b) el uso de nuevas tecnologías o tecnologías en desarrollo para productos tanto nuevos como existentes.

Las entidades financieras deberán realizar esta evaluación del riesgo antes del lanzamiento de los nuevos productos, prácticas comerciales o el uso de tecnologías nuevas o en desarrollo. Los países y las entidades financieras deben tomar medidas adecuadas para administrar y mitigar los riesgos de LA/FT vinculado a nuevas tecnologías.

Con relación a la Recomendación 15 debemos precisar que, en octubre del 2018, GAFI adoptó dos nuevas definiciones en el Glosario de Términos: "activo virtual"[31] y "proveedores de servicios de activos virtuales"[32]. Activo virtual es el término que utiliza GAFI para referirse a los criptoactivos y otros activos digitales (FATF, 2019b).

Asimismo, la Recomendación 15 también se refiere a la obligación de los países de garantizar que los proveedores de servicios de activos virtuales se encuentren registrados y regulados a efectos de una correcta supervisión, así como para la adecuada gestión y mitigación de los riesgos de LA/FT que puedan surgir de las operaciones con activos virtuales.

En junio 2019, el GAFI incorporó la Nota Interpretativa a la Recomendación 15 para aclarar las indicaciones relacionadas con los requisitos de los activos virtuales y los proveedores de servicios de activos virtuales. Ello resulta importante en la medida que los países miembros tendrán mecanismos más claros para poner en práctica las regulaciones previstas por el GAFI en sus propias jurisdicciones (FAFT, 2019b).

Con respecto a esta Nota Interpretativa a la Recomendación 15, es importante mencionar que esta aclara temas vinculados a la aplicación del enfoque basado en riesgos sobre activos virtuales y proveedores de servicios de activos virtuales, así como la supervisión sobre estos proveedores de servicios de activos virtuales en cuanto a la prevención del LA/FT y las medidas de debida diligencia y reporte de operaciones sospechosas que deben adoptar los proveedores mencionados, entre otros (FAFT, 2019b).

En ese sentido, debe quedar claro que el GAFI busca imponer obligaciones de prevención de LA/FT principalmente sobre los proveedores de servicios de activos virtuales[33] (ej. las bolsas de criptoactivos), los cuales son los nuevos intermediarios en este mercado de criptomonedas.

Así, esta Nota Interpretativa señala que se debe de identificar a los proveedores de servicios de activos virtuales y requerirles que estén registrados o autorizados ante las autoridades competentes en una jurisdicción. Esto incluiría también la adecuada supervisión y fiscalización de estos proveedores de servicios de activos virtuales, los cuales deberían cumplir con obligaciones basadas en las Recomendaciones del GAFI, principalmente las Recomendaciones del 10 al 21.[34]

3.2. Directrices del GAFI.

Adicionalmente a la incorporación de la Nota Interpretativa a la Recomendación 15, el GAFI ha emitido unas Directrices para un enfoque basado en el riesgo para activos virtuales y proveedores

[24] De acuerdo con el Glosario de Términos del GAFI, se entiende por "activo virtual" a la representación digital de valor que puede ser comercializada digitalmente, o transferida, y que puede ser utilizada con fines de pago o de inversión. Los activos virtuales no incluyen representaciones digitales de monedas fiduciarias, valores y otros activos financieros que ya están cubiertos en otras partes de las Recomendaciones del GAFI.
[32] De acuerdo con el Glosario de Términos del GAFI, se entiende por "proveedores de servicios de activos virtuales" a cualquier persona física o jurídica que no esté contemplada en las Recomendaciones y que, como empresa, lleve a cabo una o más de las siguientes actividades u operaciones por cuenta o en nombre de otra persona física o jurídica: i) intercambio entre activos virtuales y monedas fiduciarias; ii) intercambio entre una o más formas de activos virtuales; iii) transferencia de activos virtuales; iv) custodia y/o administración de activos virtuales o instrumentos que permitan el control de activos virtuales; y, v) participación y prestación de servicios financieros relacionados con la oferta y/o venta de un activo virtual por parte de un emisor.
[33] Sin embargo, la obligación de gestionar y mitigar adecuadamente los riesgos de LA/FT asociados con operaciones con criptomonedas también incluye a los sujetos obligados tradicionales, como en el caso de los bancos.
[34] Estos son: N° 10 – Debida diligencia del cliente; N° 11 – Mantenimiento de registros; N° 12 – Personas expuestas políticamente; N°13 – Banca corresponsal; N° 14 – Servicios de transferencia de dinero o valores; N° 15 – Nuevas tecnologías; N°16 – Transferencias electrónicas; N°17 – Dependencia en terceros; N° 18 - Controles internos y sucursales y filiales extranjeras; N° 19 – Países de mayor riesgo; N° 20 - Reporte de operaciones sospechosas; y, N° 21 - Revelación (*tipping-off*) y confidencialidad.

de servicios de activos virtuales. Las Directrices del GAFI fueron inicialmente emitidas en el 2015 y luego actualizadas en junio de 2019.

Estas Directrices tienen como pretensión abordar lo siguiente (FAFT, 2019b):

1) Explicar la aplicación del enfoque basado en el riesgo a las medidas de prevención de LA/FT sobre los activos virtuales;
2) Identificar las entidades que participan en operaciones o actividades relacionadas a activos virtuales; y
3) Aclarar la aplicación de las Recomendaciones del GAFI sobre las operaciones con activos virtuales y los proveedores de servicios de activos virtuales.

Asimismo, es de resaltar que parte del objetivo de las Directrices es ayudar a que las autoridades nacionales desarrollen sus respuestas regulatorias, incluyendo la modificación de las leyes que abordan los riesgos asociados al LA/FT vinculadas a activos virtuales y proveedores de servicios de activos virtuales, a fin de que estas sean efectivas dentro de la jurisdicción.

Por otra parte, también se puede identificar como objetivo de las Directrices que las compañías que estén vinculadas a operaciones con activos virtuales entiendan mejor las obligaciones de prevención y mitigación del LA/FT que les son aplicables y cómo pueden efectivamente cumplir con requerimientos del GAFI.

De esta manera, el GAFI busca que las Directrices sean lo suficientemente comprensivas para que los agentes que intervienen en el mercado de criptomonedas interioricen los riesgos de LA/FT asociados a operaciones con estos activos virtuales. Cabe señalar que el GAFI está constantemente monitoreando el desarrollo de este mercado, es por eso que en junio de 2020 publicó la revisión anual de estas Directrices.

En esta última revisión mencionada, el GAFI ha destacado el avance en la implementación de lo establecido en las Directrices y la Recomendación N° 15 con relación a activos virtuales, reconociendo que ha habido un importante avance en el desarrollo de soluciones tecnológicas para la implementación del *travel rule* aplicable a proveedores de servicios de activos virtuales (FAFT,2020).

El mecanismo de prevención de LA/FT conocido como *travel rule*, constituye uno de los mecanismos clave para la mitigación de riesgos de LA/FT en el mercado de criptoactivos. La implementación de este mecanismo obliga a los proveedores de servicios de activos virtuales a obtener, custodiar e intercambiar información sobre los ordenantes y beneficiarios de transferencias de activos virtuales.

Es más, la importancia del *travel rule* es grande en el mercado de criptomonedas que, tal como explicamos, está caracterizado en el hecho de que los usuarios pueden realizar operaciones con estos activos virtuales sin revelar sus identidades y por la posibilidad de transferir criptoactivos internacionalmente de manera muy sencilla.

Por esto último, el GAFI considera al *travel* rule como el aspecto al cual debe de ponerse mayor atención para la prevención del LA/FT en operaciones con activos virtuales, resultando necesario también promover la cooperación internacional entre supervisores de proveedores de servicios de activos virtuales a fin de lograr un marco de cumplimiento global que conlleve a la debida identificación de estos proveedores en cada jurisdicción. [35]

[35] De hecho, una de las propuestas para lograr esta finalidad es la creación de una lista global de proveedores de servicios de activos virtuales, que permita identificar a aquellos proveedores debidamente registrados y/o autorizados para operar con criptoactivos.

IV. EL ESCENARIO ACTUAL DE LA PREVENCIÓN DEL LA/FT CON RELACIÓN A LAS CRIPTOMONEDAS.

En el panorama mundial, el uso de las criptomonedas se percibe como un nuevo espacio de desarrollo tecnológico cuya complejidad exige un análisis profundo de sus características y otros elementos constitutivos que, como hemos analizado, las hacen proclives a ser usadas como medios de pago en espacios de criminalidad y como herramientas para ocultar la procedencia ilícita de activos.

Este riesgo potencial en el uso criminal de las criptomonedas ha sido objeto de debates en distintos foros, con posiciones encontradas que, por un lado, envilecen a las criptomonedas y, por el otro, buscan darles una salida regulatoria que permita incluirlas en la economía formal y el sistema financiero.

Latinoamérica no ha sido ajena a estos debates ni tampoco a conflictos que han surgido ante el crecimiento del mercado de criptomonedas en los diferentes países de la región. Así, en los últimos años se ha conocido de controversias originadas por el cierre unilateral de cuentas bancarias a proveedores de servicios de activos virtuales por razones de prevención del LA/FT. A continuación, comentaremos uno de los casos más relevantes sobre el tema.

4.1. El caso chileno.

A inicios del año 2018, tres de las *exchanges* de criptoactivos más conocidas en Chile se vieron afectadas por el cierre unilateral de sus cuentas bancarias. Estos proveedores de servicios de activos virtuales afectados fueron Buda, CryptoMarket y Orionx.

Por el otro lado, las entidades financieras que unilateralmente cerraron cuentas o rechazaron mantener relaciones contractuales con estos proveedores de servicios de activos virtuales fueron BancoEstado, Scotiabank, Banco Itaú, entre otras más. Las medidas adoptadas por los bancos en Chile significaron un portazo a toda la industria de criptomonedas en el país sureño.

Las razones aducidas por los bancos se relacionaban a la falta de regulación del mercado de criptomonedas y a la posible utilización de las criptomonedas para actos delictivos, tales como el lavado de activos y el financiamiento del terrorismo.

Este rechazo a la incipiente industria cripto en Chile por parte de las entidades financieras llevó a que las *exchanges* afectadas comenzaran una batalla legal que aún no ha sido resuelta del todo[36].

Todo comenzó con las demandas presentadas por Buda y CryptoMarket en contra de 10 bancos ante el Tribunal de Defensa de la Libre Competencia (TDLC) de Chile por abuso de posición de dominio. Por su parte, Orionx también demandó a 6 bancos por prácticas anticompetitivas en el mercado de pagos digitales.

El resultado inicial de esta controversia fue le emisión de una medida precautoria por parte del TDLC que obligó a los bancos a seguir atendiendo a las *exchanges* y permitió que estas últimas puedan seguir ofreciendo sus servicios a sus clientes.

Sin embargo, el caso de Orionx fue llevado hasta la Corte Suprema de Chile que emitió una sentencia en sentido contrario, respaldando la decisión de BancoEstado de cerrar la cuenta bancaria de Orionx.

[36] Como informaron diversos medios durante este año 2020, varios bancos han efectuado bloqueos o cierre de cuentas bancarias que tienen como titulares a proveedores de servicios de activos virtuales.

Los argumentos que respaldaban esta decisión de la Corte Suprema se fundamentaban nuevamente en la falta de regulación y a la posibilidad de que las criptomonedas o criptoactivos puedan ser usados para el lavado de activos y otros delitos. Sin embargo, cabe anotar que esta decisión de la Corte Suprema no afectó la vigencia de la medida precautoria a favor de las *exchanges* impuesta por el TDLC, manteniéndose vigente la orden de no cerrarles las cuentas bancarias a estas empresas.

Actualmente, la batalla legal entre bancos y *exchanges* todavía no ha sido resuelta. Asimismo, se viene trabajando desde hace ya un tiempo en una regulación que contemple a las criptomonedas con el fin de otorgar mayor seguridad jurídica a las operaciones con estos activos virtuales en Chile.

4.2. De-risking ¿solución o problema?

A diferencia de Chile, en el Perú no ha habido un caso relevante de cierre unilateral de cuentas bancarias o rechazo de proveedores de servicios de activos virtuales que haya sido llevado a los tribunales o autoridades competentes. Sin embargo, ello no significa que no pueda suceder más adelante.

Lo que ha venido sucediendo en el país vecino desde 2018 ha sido un claro ejemplo de lo que se conoce como *de-risking*. Este concepto en inglés está definido como el proceso aplicado por entidades financieras que tiene como propósito abandonar o reducir determinadas líneas de negocio para evitar riesgos regulatorios y de cumplimiento (ASBA, 2017, p.4; Toso Milos, 2020, p. 3).

El *de-risking* en el ámbito de la prevención del LA/FT está vinculado a la decisión de no iniciar o mantener una relación comercial con clientes que estén considerados como de alto riesgo de LA/FT (Stabile, 2014; Aguedo, 2019). Son varios los modelos de negocios o sectores que estarían dentro de esta categoría[37], incluido a los proveedores de servicios de activos virtuales.

Los motivos por los que las entidades financieras deciden dejar de ofrecer sus servicios a ciertos clientes son básicamente los siguientes: (i) percepción de alta exposición al riesgo de LA/FT[38]; (ii) incremento de costos de cumplimiento[39], (iii) poca rentabilidad[40]; y, (iv) estrictas exigencias regulatorias y sanciones[41] (Aguedo, 2019).

[37] Por ejemplo, empresas de remesas, banca corresponsal, organizaciones sin fines de lucro, etc.

[38] De acuerdo con Beatriz Aguedo (2019): "El riesgo es que el mantenimiento de las relaciones comerciales con algunas clases de empresas genere una alta exposición a las entidades del sistema financiero de ser usadas como medios para realizar actos de conversión, transferencia, ocultamiento y tenencia, o funcionar como un eslabón para la realización de actos de transporte, traslado, ingreso o salida de dinero o instrumentos valores de origen ilícito".

[39] De acuerdo con Beatriz Aguedo (2019), "Tener un cliente de alto riesgo dentro del portafolio implica la aplicación de controles mucho más exigentes, que garanticen que la institución está tomando todas las medidas necesarias para mitigar el riesgo inherente que presenta. Sin embargo, la implementación de controles no es gratis: el problema yace en el alto costo que implica garantizar la aplicación de las políticas de Conocimiento de Cliente (KYC) y los requerimientos de Debida Diligencia Reforzada (EDD) toda la relación comercial".

[40] De acuerdo con Beatriz Aguedo (2019), "En base a la expectativa de captar fondos y colocarlos, los costos de cumplimiento se asumen con la expectativa del retorno. La pregunta clave es la siguiente: ¿qué sucede con aquellos clientes de alto riesgo que, pese a requerir un esfuerzo mayor para aplicar los lineamientos del Conocimiento del Cliente, no generan mayor rentabilidad y simplemente exponen a la entidad a mayores riesgos de LA/FT? La respuesta de las entidades que efectúan estas prácticas es que, al desvincularse y cortar relaciones con un cliente, la institución financiera perderá oportunidades de negocio, pero la pérdida se compensará al no tener que lidiar con el coste de cumplimiento".

[41] De acuerdo con Beatriz Aguedo (2019), "La crisis financiera mundial de 2007-2008 marcó un antes y después, no solo en los estándares macro y micro prudenciales, sino también en el endurecimiento de la normativa nacional e internacional contra el LA/FT. Desde 2009, las instituciones financieras a nivel global han sido multadas con más de USD 17 mil millones, siendo el reciente caso del Danske Bank el más emblemático, puesto que, de determinarse la culpabilidad del banco danés

Tomar la decisión de rechazar clientes en base al *de-risking* es la solución más simple y menos costosa en el corto plazo. Sin embargo, consideramos que no es la estrategia más adecuada desde una perspectiva integral del sistema financiero y de más largo plazo.

En efecto, la estrategia que adoptan las entidades financieras es válida, pero ¿siempre resulta justificada? De acuerdo con Toso Milos (2020), la aplicación del *de-risking* es un efecto indeseado del enfoque basado en el riesgo que deben de aplicar las entidades financieras para la prevención del LA/FT.

En ese sentido, aplicar el *de-risking* resultaría una consecuencia indeseada del enfoque basado en el riesgo debido a que, contrariamente a su propósito, no permite que las entidades financieras gestionen los riesgos de LA/FT asociados con cierto sector o negocio (Toso Milos, 2020, p. 7).

Además, también resulta paradójico, ya que es la obligación de prevenir el LA/FT mediante un enfoque basado en el riesgo lo que finalmente es usado como justificación por las entidades financieras para eliminar por completo el riesgo de LA/FT mediante el *de-risking* (ASBA, 2017, p.10; Toso Milos, 2020, p. 7).

Por eso, aplicar el *de-risking* sin un adecuado análisis de gestión de riesgos y sin considerar las particulares de cada cliente conlleva a una exclusión inapropiada de usuarios del sistema financiero, lo que promueve que los usuarios excluidos busquen canales alternativos e informales, pudiendo incrementarse el riesgo de comisión de delitos de LA/FT (Stabile; 2014; ASBA, 2017, p.10; Toso Milos, 2020, p. 9).

Incluso, el rechazo o terminación de relaciones comerciales con empresas de un mismo sector -como pasó en Chile- puede traer también los siguientes efectos negativos (Stabile, 2014):

- Pérdida de ingresos: El recorte de líneas de negocio y grupos de clientes específicos tiene un impacto en los ingresos tanto en el corto como en el largo plazo, al perder la oportunidad de hacer negocios con sectores potencialmente rentables.
- Daños reputacionales y afectación de relaciones comerciales: Debido a que las estrategias de *de-risking* son difíciles de comprender por los consumidores financieros, existe una alta posibilidad de comentarios negativos en el espacio público (ej. a través de la prensa), así como de que se efectúen reclamos y demandas (ej. caso chileno).
- Transferencia del riesgo, pero no disminución: Como consecuencia de que grandes bancos cierren cuentas a clientes de alto riesgo de LA/FT, estos últimos contratarán servicios financieros con entidades financieras más pequeñas o entidades no reguladas (ej. FinTech), las cuales no suelen adoptar las medidas y controles de prevención del LA/FT al mismo nivel de los bancos más grandes.

Por ello, lo adecuado para una efectiva gestión de riesgos LA/FT consistiría en aplicar las medidas de debida diligencia reforzada con respecto a los clientes considerados de alto riesgo de LA/FT. Sin embargo, esto no siempre resulta fácil ya que implica la verificación de origen de fondos, la identificación del beneficiario final, análisis del propósito de la cuenta, evaluación del perfil del cliente, entre otras actividades.

En esa línea, hay que considerar que la recopilación y verificación de información puede ser un proceso bastante costoso, además de que puede tornarse complicado debido a otros factores atribuidos al cliente (ej. negativa de entregar información calificada como confidencial) o a terceros (ej. negativa de entidades del extranjero de entregar información de sus clientes). Incluso,

por lavar dinero a través de su sucursal de Estonia, podría recibir hasta USD 8 mil millones, sobrepasando incluso al famoso caso HSBC".

puede ser todavía más difícil si tomamos en cuenta las características de los criptoactivos, comentados anteriormente.

Así, el hecho de que los usuarios en el mercado de criptomonedas realicen operaciones de manera anónima o seudónima no se condice con los requerimientos usuales de identificación de los intervinientes de una transacción financiera, los cuales son necesarios para el conocimiento del cliente y/o de la contraparte, y que son parte de las principales obligaciones que tienen que cumplir las empresas de los sectores económicos obligados a reportar operaciones sospechosas a las Unidades de Inteligencia Financiera según su jurisdicción. Esta ausencia de divulgación de datos personales va en contra de cualquier política de prevención de LA/FT a nivel global, referido a la identificación del cliente.

Cabe resaltar que la falta de información de los usuarios no significa que las transacciones con criptomonedas efectuadas por estos no puedan ser rastreadas, puesto que el diseño de estas redes contempla que la información transaccional sea transparente y accesible al público. Sin embargo, la cuestión está en que los mismos promotores de bitcoin y otras criptomonedas recomiendan proteger la privacidad de los usuarios a través de diferentes métodos que buscan eliminar el nexo entre transacciones efectuadas, tal como se muestra en la página web bitcoin.org[42]:

> (…) Estas direcciones son creadas de forma privada por el monedero del usuario. Sin embargo, una vez que se utilizan, estas son manchadas por la historia de todas las transacciones involucradas. Cualquier persona puede ver el saldo y operaciones de cualquier dirección. Dado que los usuarios usualmente tienen que revelar su identidad para recibir bienes o servicios, las direcciones Bitcoin no pueden permanecer completamente anónimas. Es por esa razón que las direcciones Bitcoin deberían ser usadas una única vez y no ser descuidado para no revelar sus direcciones (el subrayado es nuestro).

Dicho esto y tomando en cuenta los riesgos de LA/FT asociados a las operaciones con criptomonedas, consideramos que, aunque pueda parecer incoherente desde una lógica empresarial, lo adecuado no es rechazar automáticamente a clientes que presenten alto riesgo de LA/FT, sino que la terminación de la relación contractual con este tipo de clientes debe ser aplicada solo luego de un análisis individual por cliente u operación y cuando los riesgos de LA/FT presentes no puedan ser mitigados o controlados (Toso Milos, 2020, p. 7).

En tal sentido, los costos asociados al cumplimiento de la normativa en materia de prevención del LA/FT, que comprende adoptar un enfoque basado en el riesgo y aplicar la debida diligencia reforzada en el conocimiento del cliente, no deberían ser la única justificación para decidir no mantener vínculos comerciales con un cliente o sector específico, tal como ocurrió con los proveedores de servicios de activos virtuales en Chile.

V. CONCLUSIONES.

Las criptomonedas consisten en una innovación tecnológica que viene revolucionando las finanzas tradicionales y que cada día tiene más usuarios. Sin embargo, sus características y el entorno en el que operan las hacen propicias para ser usadas en delitos de lavado de activos y

[42] Véase: https://bitcoin.org/es/proteja-su-privacidad

del financiamiento del terrorismo (LA/FT), aunque todavía no sean el medio más utilizado actualmente para cometer estos delitos.

Como respuesta a la ausencia de una regulación sobre criptomonedas en el Perú y en otros países, los bancos y entidades financieras han venido tomando acciones frente al avance de la adopción de las criptomonedas según su capacidad operativa y comprensión de este mercado, lo cual, en muchas ocasiones, ha sido insuficiente.

Por ello, resultan apropiadas las acciones que viene tomando el GAFI en cuanto al monitoreo constante de este mercado y la emisión de directrices que orienten a los sujetos obligados a cumplir adecuadamente con sus obligaciones para la prevención del LA/FT cuando tengan por cliente a un proveedor de servicios de activos virtuales.

Sin embargo, también es importante resaltar el conflicto detrás de dos ecosistemas o sistemas encontrados en la prevención del LA/FT. Bitcoin, precursor del ecosistema cripto, nació con la finalidad de ser una red que funcione sin terceros de confianza (ej. bancos) y basado fuertemente en la privacidad de sus transacciones, por lo que el control o la influencia que ejercerían las entidades financieras sobre las operaciones con criptomonedas bajo la obligación de prevenir el LA/FT contradice esta idea postulada por Satoshi Nakamoto.

A manera de reflexión final, consideramos que aún queda un largo desarrollo en la implementación de medidas de prevención del LA/FT para operaciones con criptomonedas y proveedores de servicios de activos virtuales. Aquí lo importante será encontrar en dicho desarrollo un equilibrio adecuado para no perjudicar el avance del ecosistema cripto sin descuidar la aplicación de la gestión de riesgos y controles de prevención del LA/FT cuando sea necesario.

VI. REFERENCIAS BIBLIOGRÁFICAS.

Antonopoulos, Andreas M. (2017). *Mastering Bitcoin: Programming the Open Blockchain*. (2da. ed.). Sebastopol: O'Reilly Media.

Aguedo, Beatriz. (2019). Gestión de riesgos, De-risking y Criptomonedas en el Mercado Financiero Peruano. Recuperado de https://thecryptolegal.com/gestion-de-riesgos-de-risking-y-criptomonedas/.

ASBA. (2017). Una visión general sobre el De-risking: causas, efectos y soluciones. Recuperado de http://www.asbasupervision.com/es/bibl/i-publicaciones-asba/i-2-otros-reportes/1597-una-vision-general-sobre-el-de-risking-causas-efectos-y-soluciones/file

Chainalysis. (2020). The 2020 State of Crypto Crime: Everything you need to know about darknet markets, exchange hacks, money laundering and more. Recuperado de https://go.chainalysis.com/rs/503-FAP-074/images/2020-Crypto-Crime-Report.pdf

CipherTrace (2020). Cryptocurrency, Crime and Anti-Money Laundering Report, Spring 2020. Recuperado de https://ciphertrace.com/wp-content/uploads/2020/06/spring-2020-cryptocurrency-anti-money-laundering-report.pdf

Europol. (2015). Why is cash still king? A strategic report on the use of cash by criminal groups as a facilitator for money laundering. Recuperado de https://www.europol.europa.eu/publications-

documents/why-cash-still-king-strategic-report-use-of-cash-criminal-groups-facilitator-for-money-laundering

FAFT. (2019a). The FAFT Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. Recuperado de http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf

FAFT. (2019b). Virtual Assets and Virtual Asset Service Providers: Guidance for a Risk-Based Approach. Recuperado de https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf

FAFT. (2020). 12-Month Review of the Revised FAFT Standards on Virtual Assets and Virtual Asset Service Providers. Recuperado de http://www.fatf-gafi.org/media/fatf/documents/recommendations/12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf

García Long, Sergio y Adolfo Morán Cavero. (2019). *Criptomonedas y Psicología Financiera*. En: Chipana, Jhoel (Coord.), Derecho y Nuevas Tecnologías: El impacto de una nueva era, pp. 243-262.

Stabile, Carol. (2014). De-risking. Does one bad apple spoil the bunch?". En: ACAMS Today. Recuperado de https://www.acamstoday.org/de-risking-does-one-bad-apple-spoil-the-bunch/

Toso Milos, Ángela. (2020). De-Risking: Una consecuencia indeseada del enfoque basado en el riesgo aplicado por los bancos en materia de prevención del lavado de activos y financiamiento del terrorismo. En: Revista Chilena de Derecho, vol. 47, No. 1, pp. 1-24

Villavicencio, Felipe. (2011). Evaluación de la Legislación Penal Peruana en Materia de Lavado de Activos: Efectividad, Grado de Cumplimiento y Recomendaciones. Recuperado de http://repositorio.pucp.edu.pe/index/bitstream/handle/123456789/39943/3_investigacion.pdf?sequence=4&isAllowed=y