

**Grupo de Acción contra el Blanqueo de Dinero
en África Central
(GABAC)**

INFORME DE ESTUDIO

**LOS NUEVOS MEDIOS DE PAGO Y LOS
DESAFÍOS DE LA LUCHA ANTIBLANQUEO Y
CONTRA LA FINANCIACIÓN DEL TERRORISMO
EN LA ZONA CEMAC**

Diciembre de 2016



GRUPO DE ACCIÓN CONTRA EL BLANQUEO DE DINERO EN ÁFRICA CENTRAL

El Grupo de Acción contra el Blanqueo de Dinero en África Central (GABAC) es un órgano especializado de la Comunidad Económica y Monetaria de África Central (CEMAC) cuyas misiones son:

- La lucha contra el blanqueo de dinero y los productos del crimen;
- La organización armonizada y concertada de medidas apropiadas para esta lucha en la CEMAC;
- La evaluación de la acción y de la eficacia de las medidas adoptadas;
- La asistencia de los Estados miembros en su política antiblanqueo;
- La colaboración con las estructuras existentes en África y a nivel internacional.

El GABAC es miembro asociado del Grupo de Acción Financiera (GAFI) desde octubre de 2015.

© 2017 GABAC. Todos los derechos reservados.

No se podrá realizar ninguna reproducción o traducción de esta publicación sin autorización expresa del GABAC.

Vista general

En la CEMAC (Comunidad Económica y Monetaria de África Central), los bancos, las entidades de microfinanzas (EMF) y los operadores de telefonía móvil, han introducido, durante la última década, innovaciones a nivel tecnológico y organizativo para reforzar la inclusión financiera de las poblaciones que no tienen acceso a productos financieros en la subregión. Uno de los avances más importantes en la materia fue la llegada de la moneda electrónica, materializada por los nuevos medios de pago (NMP), como instrumentos de pago.

Sin embargo, si las transacciones financieras que permiten realizar no se trazan adecuadamente, la amplia difusión de los NMP puede favorecer la realización de operaciones de blanqueo de dinero y de financiación del terrorismo.

Se desprende del presente ejercicio de tipologías, que trata de las tarjetas de prepago, los pagos realizados mediante teléfono móvil (mobile money) así como los realizados en línea en sitios de internet, que el volumen de las transacciones realizadas a través de los NMP conoce un fuerte crecimiento en la CEMAC. El desarrollo es más importante en algunos de sus Estados miembros que en otros. Por otra parte, la falta de trazabilidad de los pagos realizados por medio de los NMP, los fallos de los dispositivos reglamentarios y de vigilancia y el anonimato de los autores de ciertas transacciones representan los principales factores de riesgo de blanqueo de dinero y de financiación del terrorismo.

Se han identificado dos casos de blanqueo de dinero relacionados con el uso de los NMP en la CEMAC: uno vinculado con el blanqueo de dinero a través de tarjetas de prepago y el otro a través del uso de mobile money.

El Banco de los Estados de África Central no dispone de un dispositivo de seguimiento de las transacciones realizadas a través de los NMP, por lo tanto, el grupo de trabajo responsable de la realización de este estudio, tuvo importantes dificultades de acceso a la información que necesitaba, tanto con los bancos y los operadores de telefonía móvil como con los órganos de

supervisión y las autoridades responsables del control y de la lucha contra el blanqueo de dinero y la financiación del terrorismo.

ÍNDICE

Introducción	8
Capítulo I	13
Repaso de la literatura en materia de inclusión financiera	13
Capítulo 2	17
Evaluación de los nuevos medios de pago en la CEMAC	17
2.1	Dispositivo reglamentario relativo a los nuevos medios de pago _____ 17
2.2	Evolución de la reglamentación relativa a los nuevos medios de pago _____ 18
2.3	Disposiciones reglamentarias en materia de lucha antiblanqueo y contra la financiación del terrorismo relacionados con los nuevos medios de pago _____ 20
2.4	El mercado de los nuevos medios de pago en la CEMAC _____ 23
2.4.1	Las tarjetas de prepago _____ 23
2.4.1.1	La distribución de las tarjetas bancarias de prepago _____ 26
Un gran número de bancos en la subregión no ofrecen tarjetas de prepago. En Camerún por ejemplo, de los trece bancos presentes, solo Ecobank Cameroun, Afriland First Bank, Atlantique Bank y UBA Cameroun emiten este tipo de NMP. 26	
1.2	_____ 27
2.2	_____ ¡Error! Marcador no definido.
3.2	_____ ¡Error! Marcador no definido.
3.1	_____ ¡Error! Marcador no definido.
3.2	_____ ¡Error! Marcador no definido.
3.3	_____ ¡Error! Marcador no definido.
3.4	_____ ¡Error! Marcador no definido.
2.4.1	_____ ¡Error! Marcador no definido.
2.4.1.1	_____ ¡Error! Marcador no definido.
2.4.1.2	La demanda de tarjetas bancarias de prepago en la zona CEMAC _____ 27
2.4.2	El mobile money _____ 30
2.4.2.1	La distribución de mobile money _____ 32
2.4.2.2	La demanda de mobile money en la CEMAC _____ 34
2.4.3	Los pagos en línea _____ 37
Capítulo III	39
Los riesgos de blanqueo de dinero y de financiación del terrorismo a través de los nuevos medios de pago en la CEMAC	39
3.1.1	Riesgos relativos a los fallos del dispositivo reglamentario _____ 40
3.1.2	Riesgos relacionados con la variedad de los actores y la rapidez de las evoluciones tecnológicas _____ 41
3.2.6	Los riesgos relacionados con la realización de las operaciones _____ 46
3.3	Riesgos relacionados con el pago mediante mobile money _____ 48

3.3.1	Riesgos relativos a la conducción de actividades a través de mobile money	48
3.3.2	Los riesgos relacionados con la identificación de la clientela	48
Capítulo IV		51
Tipologías de los riesgos de blanqueo de dinero y de financiación del terrorismo relacionados con los nuevos medios de pago		51
Casos de blanqueo de dinero y de financiación del terrorismo a través de los nuevos medios de pago en la CEMAC		51
CASO 1: Fraude informático con tarjetas de prepago y blanqueo de dinero		52
CAPÍTULO V		54
Recomendaciones para reducir los riesgos de blanqueo de dinero y de financiación del terrorismo relacionados con los nuevos medios de pago		54
5.1	Mejorar el dispositivo reglamentario de regulación y de supervisión de la actividad de oferta de los NMP	54
5.2. Coordinación de las actividades de los actores implicados en la gestión		57
Conclusión		61
ANEXO 1		64
ANEXO 2		65
ANEXO 3		67
ANEXO 4		68

Introducción

Aunque un número considerable de transacciones financieras se realiza en los sistemas financieros informales, el nivel de uso de los servicios bancarios en la zona CEMAC, un 11 % de media, representa un freno para el desarrollo de los intercambios comerciales (Mayoukou, 2000, Lelart, 2002). La baja proporción de la población activa que tiene acceso a servicios bancarios no favorece una fuerte inclusión financiera, factor de crecimiento económico social y políticamente sostenible a largo plazo (Levine, 2003, Adrianaivo y Kpodar, 2012, Babajide, 2015).

En otras palabras, en los países de la CEMAC, existe una franja importante de la población excluida del sistema financiero, pero económicamente activa, que vive fuera de la economía formal, sobre todo en las zonas periurbanas y rurales, en las que la densidad de las oficinas bancarias es muy baja. Además, la población que tiene acceso a servicios financieros no siempre hace un uso sistemático de los mismos.

En este entorno los bancos, las entidades de microfinanzas (EMF) y los operadores de telefonía móvil implantados en la CEMAC han introducido, durante la última década, innovaciones a nivel tecnológico y organizativo para favorecer la inclusión financiera de las poblaciones que no tienen acceso a productos financieros en la subregión. Una de las iniciativas más importantes en la materia fue la llegada de la moneda electrónica, materializada por los NMP, como instrumento de pago.

El reglamento n.º 01/11/CEMAC/UMAC/CM define la moneda electrónica como «un valor monetario incorporado en forma electrónica a cambio de entrega de fondos de valor igual, que puede usarse para realizar pagos a personas que no sean el emisor, sin necesidad de cuentas bancarias para realizar la transacción». Los instrumentos de la moneda electrónica, objeto de este estudio, se componen de las tarjetas de prepago, los pagos por internet y los realizados a través de un teléfono móvil, designados «mobile

money». Generalmente se agrupan bajo la denominación de nuevos medios de pago (NMP).

A pesar de su adopción relativamente tardía en la CEMAC, en comparación con otras subregiones africanas¹, estos instrumentos conocen desde su introducción una evolución significativa tanto en número de instrumentos emitidos como en volumen de transacciones realizadas.

La adopción de estrategias nacionales de inclusión financiera elaboradas por varios Estados miembros de la CEMAC, así como la adopción y aplicación de textos reglamentarios que favorecen el desarrollo de la oferta y de la demanda de NMP contribuyen a la difusión de estos instrumentos financieros en la CEMAC. Sin embargo, resulta que los fallos de los sistemas financieros a la hora de controlar las transacciones financieras realizadas a través de los NMP pueden favorecer el blanqueo de dinero y la financiación del terrorismo. Dos fenómenos que constituyen una amenaza para la estabilidad financiera y la prosperidad económica de los Estados (Lawack, 2013). Pueden comprometer la integridad del sistema financiero, falsear la asignación de los recursos financieros, especialmente dando una orientación incorrecta de las inversiones en la economía por una parte, y un vector de inseguridad por el que ciertos países de la subregión pagan un elevado tributo. Por lo tanto, sería indispensable enmarcar mejor y controlar el uso de los NMP para reducir los riesgos de blanqueo de capitales y de financiación del terrorismo en un preocupante contexto de inestabilidad.

El blanqueo de capitales se define en el artículo 1 del reglamento n.º 01/CEMAC/UMAC/CM relativo a la prevención y represión del blanqueo de capitales y de la financiación del terrorismo en África Central como: *«a) la conversión o la transferencia de bienes procedentes de un crimen o de un delito, según los textos aplicables en el Estado miembro o del presente Reglamento, con el objetivo de disimular o enmascarar el origen ilícito de dichos bienes y de ayudar cualquier persona implicada en la misión de este*

¹ A menudo se presenta el ejemplo de Kenia. Este país de África del este conoce uno de los mayores desarrollos en materia de mobile money de África.

crimen o delito a escapar de las consecuencias jurídicas de sus actos». ²... Disponibles para una amplia clientela, los nuevos medios de pago podrían ser un instrumento al servicio de los delincuentes y de las personas culpables de actividades de blanqueo de capitales o de financiación del terrorismo.

Al igual que el blanqueo de capitales, la financiación del terrorismo se define en el mismo Reglamento como el *«hecho para cualquier persona de aportar o reunir por cualquier medio que sea, directa o indirectamente, de forma ilícita o deliberada, fondos con la intención de que se utilicen o sabiendo que se van a utilizar total o parcialmente con el objetivo de cometer: a) un acto que represente una infracción de terrorismo según la definición de uno de los tratados internacionales pertinentes debidamente ratificado por el Estado miembro;...»*. En vista de esta precisión, los NMP podrían representar un medio de almacenamiento, de transporte, de pago y de transferencia de fondos destinados a actividades terroristas. La coyuntura de los Estados de la CEMAC, especialmente la de Camerún, de la RCA y de la República del Chad con los movimientos insurreccionales y terroristas tales como Boko Haram, Seleka, Anti Balaka, impone ciertamente una supervisión eficaz del uso de los NMP.

Objetivos

Entre otros, y en cumplimiento de estos términos de referencia, el objetivo de este ejercicio de tipologías es hacer un balance de los desarrollos de los NMP en la subregión, hacer un análisis comparativo de los diferentes enfoques reglamentarios susceptibles de regular y de supervisar el fenómeno de los NMP, y mantener un equilibrio entre la necesidad de promover la inclusión de clases de poblaciones que no tienen acceso al sistema financiero y la lucha contra el blanqueo de dinero y la financiación del terrorismo; identificar los riesgos y las vulnerabilidades específicas inherentes a los NMP siguientes: tarjetas de débito de prepago, los sistemas de pago en línea (incluida la moneda virtual) y los servicios de pago a través

² Reglamento n.º 01/CEMAC/UMAC/CM relativo a la prevención y a la represión del blanqueo de capitales, la financiación del terrorismo y la proliferación en África Central de 16 de abril de 2016, artículo 8 a).

de los teléfonos móviles y, finalmente, basándose en estudios de casos realizados al ser posible en la subregión, definir los modos operativos y las tendencias del uso abusivo de los NMP con fines de blanqueo de dinero y de financiación del terrorismo en África Central.

Metodología

Teniendo en cuenta los desarrollos anteriores, tras un seminario taller organizado sobre el tema, el Grupo de Acción contra el Blanqueo de Dinero en África Central (GABAC) constituyó un grupo de trabajo al que se encargó la tarea de llevar a cabo un ejercicio de tipologías relativo a cinco de los seis Estados de la CEMAC³ y con el objetivo de detectar y frenar las vulnerabilidades al blanqueo de dinero y a la financiación del terrorismo inherentes al uso de los NMP.

Este grupo se componía de cuarenta miembros procedentes de autoridades nacionales responsables de la regulación y de la supervisión del sector financiero, de las actuaciones penales y de las investigaciones de la policía judicial (Finanzas, Justicia y Seguridad), de las entidades de crédito, de las compañías de telefonía móvil que ofrecen los NMP en los Estados de la subregión, de células de información financiera, así como de autoridades regionales responsables de la supervisión y del control del sistema financiero en África Central (Banco de los Estados de África Central y Comisión Bancaria de África Central).

La información se recopiló de organismos subregionales de regulación y de supervisión, células de información financiera, autoridades nacionales de supervisión y de control del sector financiero, autoridades judiciales, entidades de crédito y operadores de telefonía móvil.

El grupo de trabajo realizó cuestionarios que remitió a las administraciones y entidades anteriormente mencionadas. Los resultados de las encuestas revelan que tres (03) cuestionarios fueron cumplimentados respectivamente por los agentes de la autoridades responsables del control y

³ Guinea Ecuatorial no participó en los trabajos.

de la lucha contra el blanqueo de dinero y por la autoridades de control y de supervisión. Por otra parte, diez (10) cuestionarios fueron cumplimentados por los agentes de banco y de compañías de telefonía móvil. Los datos extraídos de los cuestionarios se completaron con entrevistas semidirigidas con los actores del sistema financiero. Trece (13) entrevistas fueron llevadas a cabo con las autoridades de regulación y de control y otras once (11) con agentes de banco y de compañías de telefonía móvil. El procesamiento de estos datos condujo a la formulación de propuestas.

El presente informe de estudio se compone de cinco capítulos: el primero consiste en un breve repaso de los escritos acerca de los NMP; el segundo está dedicado a la evaluación de los NMP en la CEMAC; el tercero ofrece una cartografía de los riesgos relacionados con los NMP; el cuarto está dedicado al estudio de casos de tipologías; y finalmente, el quinto trata de las recomendaciones.

Capítulo I

Repaso de la literatura en materia de inclusión financiera

Más de mil millones de personas viven con menos de 500 FCFA⁴ al día y más de tres mil millones con menos de 1000 FCFA. 825 millones de personas, entre las cuales 200 millones son niños, sufren hambre en el mundo, principalmente en los países del sur (Attali, 2006). La mayoría de estas personas viven al margen de los sistemas financieros clásicos. Sin embargo, la inclusión financiera puede representar una solución al problema de financiación de estos individuos y una vía de mejora de sus condiciones de vida (Mosley y Hulme, 1996, Helms, 2006).

Desde hace tiempo, las microfinanzas se presentan como el principal instrumento de lucha con la pobreza y de inclusión financiera de las personas excluidas en los países subdesarrollados. Al acceder a servicios de microfinanzas, y especialmente al microcrédito, sus beneficiarios, en gran mayoría pobres, pueden realizar actividades generadoras de ingresos (Armandariz de Aghion y Morduch, 2005, Lelart, 2005). Con los ingresos que realizan, pueden satisfacer necesidades elementales como vestirse, alimentarse, recibir asistencia médica, pagar los gastos de escolaridad de los niños, entre otras cosas.

Sin embargo, el difícil acceso a las microfinanzas para las personas desamparadas, que deriva de la búsqueda del beneficio para algunas EMF, cuestiona la elección de los pobres por estas instituciones (CGAP, 2001). Reduce las posibilidades de las microfinanzas para servir a los más pobres y garantizar una inclusión financiera de los indigentes (Helms, 2006). Las microfinanzas en África Central son más bien comerciales y presentan límites para contribuir a la inclusión financiera de la totalidad de sus poblaciones (Servet et al., 2010).

⁴ Un euro = 655,96 FCFA.

Según el estudio⁵ llevado a cabo por la Asociación GSM, esta estima que en numerosos países en desarrollo los operadores móviles han logrado llegar mejor a los consumidores que no usan servicios bancarios que los bancos. Los servicios de dinero móvil aportan una ocasión única de permitir que los clientes que disponen de un teléfono móvil, pero no de una cuenta bancaria, pasen de un sistema de pago con dinero en efectivo a un sistema financiero formal que les da acceso a una gran variedad de servicios financieros.

Estudios conducidos en varios países, especialmente en Brasil, en Sudáfrica, en Kenia, en Malasia y en Filipinas indican que el coste reducido de los servicios de dinero móvil representa uno de los factores determinantes de su adopción. La velocidad de ejecución, su facilidad de uso, así como el sentimiento de seguridad del cliente para su dinero y las transacciones que realiza también son factores importantes.

La investigación demuestra que los servicios de dinero móvil permiten que la clientela pase de una economía basada en dinero en efectivo al sector financiero formal. Cuando se establece la confianza, los clientes que anteriormente no usaban servicios bancarios están dispuestos a suscribir servicios financieros tradicionales, tales como cuentas de ahorro (por ejemplo, los clientes que anteriormente no usaban servicios bancarios formulan una solicitud de cuenta de ahorro tras haberse convertido en usuarios hábiles de servicios de dinero móvil. Después, los bancos pueden tomar el relevo y hacerse cargo de estos nuevos clientes). Por lo tanto, el dinero móvil tiene una función importante de introducción de los clientes que no usan servicios bancarios en el sistema financiero formal. A gran escala, esto se traducirá en una formalización del sistema financiero y en una reducción global del riesgo de BC/FT».

Desde su aparición, el mobile money y el resto de NMP han facilitado el acceso a servicios financieros a personas que se encontraban al margen de los sistemas financieros clásicos (Klein y Mayer, 2011, Donovan, 2012,

⁵ El dinero móvil al servicio de las personas que no usan servicios bancarios (Maria solin, Andrew Zerzan, 2009).

Lal y Sachdev, 2015). Con estos nuevos instrumentos, miles de millones de personas realizan transacciones financieras en el mundo (Châtain et al., 2008). Debido en parte al dinamismo de las microfinanzas, en Camerún, la tasa de uso de servicios bancarios se sitúa alrededor del 20 % (superior a la tasa media de la zona CEMAC). Con respecto al uso del teléfono móvil, en ese mismo país, la tasa de penetración de este pasó del 9,8 % en 2004 al 71 % en 2014, con un número de abonados del orden de 18,6 millones y un mercado potencial de cerca de 15 millones para el mobile money⁶. En Gabón, el número de abonados se acercaba a los tres millones en 2014⁷, mientras que era de 4,59 millones en la República del Congo en 2015⁸. En Chad, la tasa de penetración del teléfono móvil pasó del 0,07 % en 2000 al 39,75 % en 2014. Los NMP, y en especial el mobile money, favorecen en estos países un acceso fácil a los servicios financieros a una amplia categoría de población que no dispone de una cuenta bancaria.

Sin embargo, sería necesario reconocer que el uso de los NMP expone al sistema financiero a importantes riesgos de blanqueo de dinero y de financiación del terrorismo. Estos son altamente tributarios de varios factores que determinan su incidencia (Di Castri, 2013). Uno de los factores principales de estos riesgos son los fallos de la tecnología, que conduce a las organizaciones a emplear procesos automatizados. Y estos procesos son poco eficaces para frenar los riesgos indicados, ya que los fenómenos estudiados son muy complejos y evolutivos. El uso de estos medios de movilización de la moneda electrónica, que no siempre está conectado a una institución financiera y puede pasar rápidamente de un actor a otro, dificulta el conocimiento de las identidades de las múltiples personas implicadas (Demetis, 2010, P09). La falsa identidad de los usuarios, el carácter fragmentado de las transacciones y la rapidez de estas, que se pueden realizar en cualquier lugar y en cualquier momento, son algunos de

⁶ Estas estadísticas han sido extraídas del Diario «Investir au Cameroun» n. ° 38 de junio de 2015. Varios artículos de este número están dedicados al uso de mobile money en el país.

⁷ <http://www.lenouveaugabon.com/telecom/1006-9149-gabon-1-million-d-internautes-3-millions-d-abonnes-au-mobile>

⁸ <http://www.afrique-it.com/web-tech/analyse-comparative-de-la-telephonie-mobile-au-congo-brazzaville-arpe/>

los factores que favorecen la aparición de estos riesgos (Chatain et al., 2008).

La combinación de estos diferentes factores de riesgo en contextos variados ha dado lugar a casos de tipologías de blanqueo de dinero y de financiación del terrorismo. Un estudio del contexto francés⁹ permitió identificar varios casos de blanqueo de dinero a través de los NMP. Estos casos tuvieron que ver con (1) el ejercicio ilegal de la profesión de banquero usando una moneda virtual que no tiene circulación legal (bitcoin), (2) la complejidad de la detección del origen de los fondos y la distribución de tarjetas de prepago por parte de un actor opaco, (3) el uso de tarjetas de prepago en un esquema fraudulento.

Por otra parte, un estudio del contexto coreano que trataba exclusivamente de mobile money condujo a la identificación de una tipología de casos de blanqueo de dinero. Uno de estos casos concierne el juego cibernético. Consiste en que una persona que usa una falsa identidad participa en juegos ilegales de dinero en internet. Para ello, contrata a empleados extranjeros y cómplices para permitirle depositar sus ganancias, procedentes del juego, en los bancos coreanos. Otro caso trata de las transferencias de dinero transfronterizas: una persona que también usa falsas identidades abre varias cuentas en bancos. Estas cuentas le servirán después para recibir importantes cantidades de dinero durante un corto periodo de tiempo. Los fondos que le envían múltiples personas cuyas identidades son falsas se usan después para la realización de transacciones con mobile money. Un último caso concierne una estafa a través del canal de un fondo de inversión, creado con fines fraudulentos. Los inversores, atraídos por la promesa de un retorno de la inversión elevado, envían importes considerables de dinero al fondo de inversión con mobile money (Chatain et al., 2008, p.15).

Los estudios llevados a cabo en Europa y en Asia muestran que las tipologías de blanqueo de dinero y de financiación del terrorismo son

⁹ TRACFIN, Monedas electrónicas, monedas virtuales y nuevos riesgos.

tributarias de la zona en la que se realizan las transacciones. Este enfoque contingente del fenómeno exige por lo tanto un análisis especial en el marco de la CEMAC para entender mejor qué forma pueden tomar ahí el blanqueo de dinero y la financiación del terrorismo a través de los NMP.

Capítulo 2

Evaluación de los nuevos medios de pago en la CEMAC

Antes de tratar los fenómenos de blanqueo de dinero y de financiación del terrorismo relacionados con los NMP en la CEMAC, resultaba conveniente realizar una evaluación de su misión y de su difusión en la Subregión para conocer los intervinientes, los usuarios, el tipo de transacciones financieras que permiten realizar y el dispositivo reglamentario y de supervisión que se aplica a estos medios de pago.

2.1 Dispositivo reglamentario relativo a los nuevos medios de pago

El dispositivo reglamentario que rige los NMP en la CEMAC se inscribe en el marco del proyecto de modernización de los sistemas y medios de pago puestos en marcha por el Banco de los Estados de África Central (BEAC) en 1999, con el objetivo de modernizar estos sistemas y limitar el uso del dinero efectivo en la Subregión. En el marco de este proyecto, se formó un dispositivo reglamentario con los reglamentos y las instrucciones siguientes:

- Reglamento n.º 01/03/CEMAC/UMAC/CM de 4 de abril de 2003 sobre la prevención y represión del blanqueo de capitales y la financiación del terrorismo en África Central;
- Reglamento n.º 02/03/CEMAC/UMAC/CM de 4 de abril de 2003 relativo a los sistemas y medios de pago;
- Reglamento COBAC R-2005/01 relativo a las diligencias de las entidades con obligaciones en materia de lucha contra el blanqueo de capitales y la financiación del terrorismo en África Central;

- Reglamento COBAC R-2005/02 relativo a las entidades de moneda electrónica;
- Reglamento n.º 01/11/CEMAC/UMAC/CM de 18 de septiembre 2011 que determina las condiciones de ejercicio de la actividad de emisión de moneda electrónica, así como las funciones de las autoridades de regulación;
- Instrucción n.º 01-GR de 31 de octubre de 2011 del Gobernador de la BEAC relativa a la vigilancia de los sistemas de pago mediante moneda electrónica, con un marco de referencia en anexo que recopila los elementos que permiten a la BEAC garantizar su misión de vigilancia de la actividad;
- Instrucción n.º 02/GR/UMAC de 7 de mayo de 2014 del Gobernador de la BEAC relativa a la puesta en marcha del multibanking en el marco de la actividad de emisión de moneda electrónica.

2.2 Evolución de la reglamentación relativa a los nuevos medios de pago

La modernización progresiva de los sistemas y de los medios de pago en la subregión de África Central condujo a la adopción de la moneda electrónica, cuyos diferentes soportes se agrupan bajo la denominación de NMP e incluyen las tarjetas de prepago, la telefonía móvil (mobile money) y los pagos por Internet.

La reglamentación que rige la moneda electrónica trata primero los textos comunitarios relativos a los medios de pago. Después, se completa con el Reglamento n.º 01/11/CEMAC/UMAC/CM, la Instrucción n.º 01/GR del Gobernador de la BEAC, así como con la Instrucción n.º 02/GR/UMAC de 7 de mayo de 2014. Estos textos tratan:

- las definiciones;
- el objeto y el campo de aplicación;
- las condiciones de ejercicio de la actividad de emisión de moneda electrónica;

- el régimen de emisión de moneda electrónica y su conversión a moneda fiduciaria o escritural;
- la regulación del control y la vigilancia de la actividad de emisión de moneda electrónica;
- el cese de la actividad de emisión de moneda electrónica;
- las disposiciones transitorias y finales.

Definen la moneda electrónica como un valor monetario incorporado en forma electrónica a cambio de la entrega de fondos de valor igual, que puede usarse para realizar pagos a personas que no sean el emisor, sin necesidad de cuentas bancarias para realizar la transacción. Por lo tanto, la moneda electrónica se caracteriza principalmente por ser:

- una deuda de la que dispone el poseedor ante el emisor y de la que puede pedir el reembolso en cualquier momento del importe o del valor en su posesión no utilizado;
- un instrumento electrónico, ya que los dispositivos electrónicos (tarjetas de prepago, mobile money, servidor de ordenador) facilitan el almacenamiento y la gestión a distancia, así como su uso en las transacciones financieras y comerciales;
- un medio de intercambio que puede usarse con fines de pago a favor de terceros diferentes del emisor de la moneda electrónica, o de transferencia de fondos entre particulares, o incluso de retirada de efectivo en un cajero automático de billetes.

Atribuyen la exclusividad del ejercicio de la actividad de emisión de moneda electrónica solamente a las entidades de crédito. Por otra parte, determinan el contenido de los contratos celebrados entre los establecimientos emisores y los portadores, los aceptadores, y asignan la regulación y el control de esta actividad a la COBAC y a la BEAC. También introducen para estas entidades de crédito una obligación de información y

comunicación y extienden el control de esta actividad a los socios técnicos y comerciales. (Ndjimba¹⁰, 2016).

Este dispositivo reglamentario describe la función de los intervinientes en la actividad de la moneda electrónica y las condiciones de su ejercicio. Se completa con disposiciones acerca del multibanking con el objetivo de garantizar la interoperabilidad en las transacciones mediante moneda electrónica en la CEMAC. El marco jurídico de la CEMAC relativo a los NMP se asemeja, en grandes líneas, al de la CEDEAO. Y esto, especialmente, con respecto a las condiciones de obtención de la autorización para ejercer y las condiciones de ejercicio en sí (Ndjimba, 2016). Sin embargo, el uso de los NMP conlleva riesgos de varios tipos, entre los cuales los de blanqueo de capitales y de financiación del terrorismo, que la reglamentación vigente, con la aportación adicional de los reglamentos adoptados por la COBAC, trata de abarcar.

2.3 Disposiciones reglamentarias en materia de lucha antiblanqueo y contra la financiación del terrorismo relacionados con los nuevos medios de pago

El dispositivo reglamentario recomienda el uso de procesos y de diligencias de lucha antiblanqueo de dinero y contra la financiación del terrorismo para paliar las vulnerabilidades relacionadas con el uso de los NMP. Por lo tanto, el reglamento n.º 01/CEMAC/UMAC/CM de 16 de abril de 2016 relativo a la prevención y a la represión del blanqueo de capitales y de la financiación del terrorismo en África Central y los reglamentos de la COBAC prevén la adopción de diligencias tales como:

- el conocimiento de los clientes (Know Your Customer, o la sigla «KYC»): por ese motivo, cualquier entidad obligada debe, antes de establecer una relación de negocios, tomar medidas de vigilancia («obligación de diligencia») con respecto a sus nuevos clientes. Consisten en la comprobación de la identidad del cliente, exigiéndole que presente un documento oficial original en curso de validez, así

¹⁰ El documento mencionado ha sido redactado por el doctor Ndjimba, en el marco de su colaboración con el GABAC. Figura un listado en anexo del presente informe.

- como la vigilancia de la procedencia de los fondos y la identificación de los beneficiarios y de las personas que controlan estos fondos;
- el conocimiento de las relaciones de negocio del cliente: con el objetivo de estimar la cantidad de sus relaciones comerciales. Esta diligencia debe realizarse cada vez que se producen cambios importantes en la actividad del cliente. Por lo tanto, el obligado puede apreciar la legitimidad de las operaciones realizadas y detectar las sospechosas, dado el caso;
 - el control de las transacciones: las entidades obligadas deben ejercer una vigilancia constante de sus relaciones de negocio y garantizar un atento examen de sus transacciones durante la duración de la relación. De ese modo se garantiza la coherencia de las transacciones realizadas por los clientes con el conocimiento actualizado de estos que las entidades obligadas deben realizar. Esta diligencia está facilitada por el uso de sistemas informatizados que permiten la detección de operaciones atípicas, teniendo en cuenta el perfil del cliente;
 - La declaración de sospecha: las entidades obligadas tienen la obligación de designar al menos a un responsable ANIF (Agencia Nacional de Investigación Financiera) y COBAC, cuya identidad se debe comunicar; también deben declarar por escrito, o en caso necesario, de forma verbal, antes o después de la ejecución, cualquier operación objeto de sospecha. Cualquier dirigente o agente no oficialmente señalado como obligado está autorizado a declarar las sospechas de blanqueo de capitales y de financiación del terrorismo en caso de emergencia;
 - La centralización de la información acerca de la identidad de los clientes, ordenantes, beneficiarios y acerca de las transacciones. A través de esta diligencia, se ha previsto la creación en cada Estado miembro de la CEMAC de archivos nacionales que se componen, entre otras cosas, del archivo de los incidentes de pago por cheque y por tarjeta de pago, así como uno de cheques y tarjetas irregulares. La información contenida en estos archivos está reservada a las

entidades obligadas para fines de perfilación de su clientela, a los oficiales de policía judicial, a los magistrados en el marco de un procedimiento judicial, a las células de información financiera y a las autoridades subregionales y nacionales de supervisión y de control;

- La comunicación de la información: la BEAC y los demás obligados deben comunicar cualquier información útil para la represión de la criminalidad financiera a las células de información financiera, a las autoridades judiciales habilitadas y a los ministerios fiscales.

Un análisis comparado más exhaustivo de los marcos jurídicos de la CEMAC y de la CEDEAO permite identificar numerosas debilidades. Estas están relacionadas con la supervisión jurídica de la actividad de emisión de moneda electrónica y las medidas relativas a la lucha contra el blanqueo de capitales a través de los NMP (Ndjimba, 2016).

A nivel de la supervisión jurídica de la actividad de la oferta de los NMP, lo esencial de las disposiciones en la CEMAC es que tienden a marcar principios genéricos sin formular reales obligaciones restrictivas. También se observa una ausencia de disposiciones relativas a las relaciones entre las entidades de crédito y sus socios, una ausencia de obligación de control interno y una falta de precisión de la responsabilidad de las entidades emisoras con respecto a las actividades de sus socios. Además, el carácter limitado de la obligación de trazabilidad, que solo es de tres (03) años en la CEMAC mientras que es de diez (10) años en la CEDEAO, representa una insuficiencia.

El marco jurídico de la CEMAC se caracteriza por una cierta vacuidad con respecto a la lucha contra el blanqueo de capitales y la financiación del terrorismo a través de los NMP. Al contrario que el de la CEDEAO, no indica claramente la obligación de los diferentes actores con las reglas comunitarias relativas a estos fenómenos.

De lo anterior se desprende que si bien el dispositivo jurídico de la CEMAC tiene el objetivo de supervisar el uso de la moneda electrónica en la subregión, no tiene en cuenta de forma adecuada los objetivos de lucha

contra el blanqueo de capitales y la financiación del terrorismo tal y como lo prevé el Reglamento 01/CEMAC/UMAC/CM de 16 de abril de 2016 para la prevención y la represión del blanqueo de capitales, la financiación del terrorismo y la proliferación en África Central.

Dicho esto, el control de los riesgos de blanqueo de capitales y de financiación del terrorismo inherentes al uso de los NMP exige, además de un marco reglamentario adecuado, un conocimiento profundo de la oferta y de la demanda de estos instrumentos en la Subregión CEMAC.

2.4 El mercado de los nuevos medios de pago en la CEMAC

Desde hace unos años, los NMP son objeto de un uso creciente en la CEMAC. Este mercado, a pesar de que incluye varios actores, permanece sin embargo embrionario, a semejanza del de las tarjetas bancarias tradicionales, todavía poco desarrollado.

2.4.1 Las tarjetas de prepago

En el sistema bancario de la Subregión circulan dos tipos de tarjetas bancarias: las tarjetas de débito, vinculadas a una cuenta bancaria, y las tarjetas de prepago. Pero solo las tarjetas de prepago serán objeto de este estudio.

Las tarjetas de débito están asociadas a una cuenta bancaria. Permiten a sus portadores retirar dinero en efectivo de los cajeros automáticos de billetes y realizar pagos, o bien en comercios equipados de terminales de pago electrónico (TPE), o bien en línea con proveedores y bancos que ofrezcan este tipo de pago. Estas tarjetas, que se presentan en forma de soporte de plástico con un microchip, son personales y funcionan generalmente mediante la introducción de un código confidencial. El uso de algunas tarjetas bancarias puede estar limitado a un país o a una red bancaria. Sin embargo, las tarjetas vinculadas a los circuitos de pago internacionales tales como VISA o MASTERCARD, pueden usarse en todo el mundo, siempre y cuando se haya activado la función que lo permite.

La gran mayoría de los bancos de la subregión CEMAC todavía no han adoptado el uso de las tarjetas de prepago en los productos que ofrecen a sus clientes por lo que siguen ofreciendo tarjetas de débito cuyo crecimiento es proporcional a la tasa de uso de los servicios bancarios por parte de los beneficiarios.

El caso del banco Crédit du Congo ilustra esta tendencia.

Durante los diez últimos años, este banco ha emitido de media 26 729 tarjetas de débito al año. Entre 2004 y 2013, el número anual de las tarjetas emitidas es casi estable. Con un aumento importante en 2014, cuando la emisión de tarjetas de prepago conoce un aumento de cerca del 25 %, el número de tarjetas emitidas ese año es de 33 397.

A diferencia de las tarjetas de débito, las tarjetas de prepago no están vinculadas a una cuenta bancaria.

La tarjeta de prepago en la zona CEMAC es un instrumento de pago electrónico según el Reglamento n.º 01/11-CEMAC/UMAC/CM de 18 de septiembre de 2011. Se trata de un conjunto de *«señales registradas en una memoria informática incorporada a una tarjeta nominativa suministrada por un emisor a un portador¹¹»*. El auge de las Tecnologías de la Información y de la Comunicación (TIC) (principalmente de la telefonía) y la firme voluntad de los países en vías de desarrollo de reducir el fenómeno de exclusión financiera han favorecido el desarrollo y la expansión de la oferta de las tarjetas de prepago.

La tarjeta de prepago funciona como una tarjeta de débito tradicional. En efecto, el portador solo puede realizar pagos o retirar dinero en función del valor monetario almacenado. Sin embargo, a diferencia de la tarjeta de débito, el hecho de tener una tarjeta de prepago no está subordinado a la posesión de una cuenta bancaria. Pero si está vinculada a una cuenta de moneda electrónica o monedero electrónico y solo puede ser emitida por una

¹¹ Reglamento n.º 01/11-CEMAC/UMAC/CM relativo al ejercicio de la actividad de emisión de moneda electrónica, artículo 1.

entidad expresamente habilitada. En África Central, solo las entidades de crédito están autorizadas a emitir moneda electrónica.

Al igual que con un monedero electrónico, el portador de la tarjeta debe cargarla con un importe. Cada vez que realiza una operación de compra o de retirada, los importes y los gastos asociados se restan del saldo. Cuando el saldo se agota, el portador debe cargar de nuevo la tarjeta para realizar nuevas transacciones. El uso de la tarjeta de prepago se extiende casi a todos: las personas sin cuenta bancaria, las personas con inhabilitación bancaria, los menores de edad, los viajeros e incluso los titulares de cuentas bancarias que no desean comunicar sus datos bancarios.

Además, otras funciones pueden asociarse a una tarjeta de prepago según los emisores. Es el caso de servicios tales como la transferencia de dinero (tarjeta a tarjeta y puesta a disposición), el pago de facturas o incluso la compra de crédito de comunicación. En el mercado bancario camerunés, algunos bancos emisores de moneda electrónica ofrecen incluso a las empresas la oportunidad de pagar los salarios de sus empleados que no disponen de una cuenta bancaria directamente a una tarjeta de prepago creada para ello. Todas estas funciones solo están disponibles dentro de una plataforma específica, que usa tecnologías concretas, la mayoría afiliadas a redes internacionales Visa y MasterCard. Las infraestructuras de programas y materiales varían según la solución de prepago utilizada por una entidad emisora.

La tarjeta de prepago ofrece varias ventajas y sobre todo es una alternativa a la cuenta bancaria. Permite que su titular se beneficie de servicios financieros básicos (reintegros, pagos, consulta de saldo) y disfrutar de la posibilidad de almacenar su dinero en efectivo de una forma más segura. Después, es factor de inclusión financiera ya que permite que los excluidos del sistema financiero formal tengan acceso a ciertos productos o servicios financieros. Finalmente, mejora la celeridad y la seguridad de las transacciones financieras y comerciales.

Aunque no se puedan rebatir las ventajas y los beneficios de este producto, su uso puede favorecer algunos comportamientos reprehensibles con respecto a las leyes y los reglamentos dictaminados por los Estados miembros de la CEMAC.

2.4.1.1 La distribución de las tarjetas bancarias de prepago

Un gran número de bancos en la subregión no ofrecen tarjetas de prepago. En Camerún por ejemplo, de los trece bancos presentes, solo Ecobank Cameroun, Afriland First Bank, Atlantique Bank y UBA Cameroun emiten este tipo de NMP.

A partir de los resultados de las entrevistas semidirigidas estudiados en profundidad, se desprende que la distribución de las tarjetas implica al fabricante del soporte de la tarjeta, al que la personaliza, a un proveedor de servicios, al banco y al cliente. Los bancos, y a veces EMF, son emisores y compradores de tarjetas. Realizan el enrutamiento de los datos y la conectividad de estos instrumentos con los cajeros automáticos y a los TPE. Además garantizan el «clearing» de las operaciones y el archivado.

En principio¹², la adquisición de una tarjeta bancaria de prepago se hace en la caja del banco. Para obtener una, el cliente debe cumplimentar una ficha de suscripción e identificarse. La personalización de la tarjeta se hace después de confirmar que el cliente no aparece en una «black list» del banco y de la firma del contrato de suscripción por el gestor.

En los bancos estudiados, los flujos de banca electrónica relativos al uso de tarjetas de prepago convergen hacia una plataforma localizada en el proveedor de servicios (ejemplo: Atos Cardamone). Este proveedor tiene una función de intermediario entre los emisores de las tarjetas y el banco en materia de flujos de banca electrónica. Por otra parte, el funcionamiento de los cajeros automáticos del banco está vinculado a la plataforma de la banca electrónica del proveedor y este realiza la compensación de los flujos de banca electrónica.

¹² Algunas entidades de crédito autorizan a los distribuidores a emitir tarjetas de prepago.

2.1.1.1 La demanda de tarjetas bancarias de prepago en la zona CEMAC

Para poder usar las tarjetas de prepago, sus portadores deben disponer de una provisión de unidades monetarias. El importe de los reintegros en efectivo y de los pagos que se pueden realizar está limitado por la reglamentación. La síntesis de los límites reglamentarios se presenta en la siguiente tabla:

Tabla 1: Límites de las transacciones a través de los NMP

REFERENCIA	ELEMENTOS DE VALORACIÓN	NORMA O ESTÁNDAR (En FCFA) ¹³
REM CP1	Límite del instrumento electrónico	5 000 000 FCFA
REM CP2	Límite de carga diaria (en efectivo)	2 000 000 FCFA
REM CP12	Límite de carga diaria (por transferencia bancaria)	5 000 000 FCFA
REM CP3	Límite por operación de retirada (cash out manual o en cajero)	500 000 FCFA
REM CP4	Límite por operación de transferencia	1 000 000 FCFA
REM CP5	Límite por operación de pago	1 000 000 FCFA
REM CP6	Límite de reintegros diarios	750 000 FCFA
REM CP7	Límite de transferencias diarias	1.500 000 FCFA
REM CP8	Límite de pagos diarios	2 500 000 FCFA
REM CP9	Límite de las transacciones diarias (retirada + transferencia + pago)	3 000 000 FCFA
REM CP10	Límite de las transacciones semanales (retirada + transferencia + pago)	5 000 000 FCFA
REM CP11	Límite de las transacciones mensuales (retirada + transferencia + pago)	10 000 000 FCFA

Fuente: BEAC

De las investigaciones se desprende que en la CEMAC las personas físicas son las principales solicitantes de las tarjetas de prepago. Estas sirven sobre todo para realizar retiradas de dinero en los cajeros automáticos de los bancos y pagos con los TPE disponibles en los comercios.

¹³ Un euro = 655,96 FCFA.

En los bancos, la recarga de las tarjetas de prepago se hace, o bien con la entrega de dinero en efectivo en las oficinas, o bien mediante débito en una cuenta bancaria. También se puede realizar desde la web del banco, mediante débito en la cuenta bancaria del cliente.

La información disponible acerca de las tarjetas de prepago se ha recopilado de¹⁴:

- UBA, Afriland First Bank Cameroun;
- UBA en Gabón;
- UBA en Congo

Sin embargo, solo los bancos que ejercen su actividad en Camerún han aportado datos lo suficientemente detallados.

Por lo tanto, la evolución anual del número de tarjetas de prepago para el banco Afriland First Bank pasó de 12 773 en 2013 a 16 326 en 2014 (es decir un aumento del 27,81 %) y a 20 322 en 2015. Durante el mismo periodo para UBA Cameroun, este número pasó de 2555 a 50 050 (es decir un progreso del 1859 % entre 2013 y 2014) y a 145 850 en 2015. En lo que se refiere a Ecobank Cameroun, permaneció casi estable.

Siguiendo con la evolución anual, en Afriland First Bank, el número de tarjetas de prepago activas representa de media el 96,9 % del número total de tarjetas. Y el volumen de las transacciones en valor a través de las tarjetas pasó de 4 385 700 062 FCFA (6 685 926 €) a 4 718 154 598 FCFA (7 192 750 €) entre 2013 y 2014, es decir un aumento del 7,58 %. Y a 5 752 463 745 FCFA (8 769 534 €) entre 2014 y 2015 es decir, un 21,9 % en valor relativo.

En lo que se refiere a UBA Cameroun, el volumen de transacción en valor a través de las tarjetas de prepago pasó de 56 387 500 000 FCFA

¹⁴ No todos los bancos de la zona CEMAC que ofrecen tarjetas de prepago han puesto a disposición del Grupo de Trabajo la información relativa a esta actividad. Además, la BEAC no dispone de información global y detallada sobre este tema, las estadísticas presentadas en este informe son parcialmente representativas de la situación real del mercado de las tarjetas de prepago en la zona CEMAC.

(85 961 796 €) en 2013 a 125 125 000 000 FCFA (190 750 960 €) en 2014, es decir un aumento del 121,9 %. Entre 2014 y 2015, este volumen de transacción conoció un crecimiento del 45,7 % llegando a 182 312 500 000 FCFA (277 932 343 €).

En Ecobank, entre 2013 y 2014, este volumen de transacción pasó de 105 132 292 000 FCFA (160 272 412 €) a 178 006 239 000 FCFA (271 367 520 €), es decir un aumento del 69,31 %. Entre 2014 y 2015, este importe aumento en un 7,15 %, llegando a 190 735 811 000 FCFA (290 773 540 €). Para todos estos bancos, se desprende que el volumen de las actividades relacionadas con las tarjetas de prepago aumenta a lo largo del tiempo.

Tabla 2: Oferta de las tarjetas de prepago para algunos bancos en África Central

Fuente: datos de investigación

Estadísticas sobre las tarjetas de prepago – Afriland First Bank Cameroun

Indicadores	2013	2014	2015	2016 (a 30/06/2016)
Número de tarjetas de prepago registradas	12 773	16 236	20 322	21 970
Número de tarjetas de prepago activas	12 339	15 737	19 750	21 390
Número de cajeros automáticos	61	78	85	102
Número de TPE	195	208	219	266
Número de transacciones realizadas	371 074	385 498	407 347	204 219
Valor de las transacciones realizadas	4 385 700 052	4 718 154 598	5 752 463 745	3 067 926 896
Saldo en curso de las tarjetas de prepago	489 977 408	522 919 184	687 069 366	700 021 527

Estadísticas sobre las tarjetas de prepago - UBA Cameroun

Indicadores	2012	2013	2014	2015
Número de tarjetas de prepago registradas	2555	2555	50 050	145 850
Número de tarjetas de prepago activas				
Número de cajeros automáticos				
Número de TPE				
Número de transacciones realizadas				
Valor de las transacciones realizadas	12 775 000 000	56 387 500 000	125 125 000 000	182 312 500 000
Saldo en curso de las tarjetas de prepago				

Estadísticas sobre las tarjetas de prepago - Ecobank Cameroun

Indicadores	2012	2013	2014	2015
Número de tarjetas de prepago registradas	1	7422	7321	8158
Número de tarjetas de prepago activas				
Número de cajeros automáticos				

Número de TPE				
Número de transacciones realizadas				
Valor de las transacciones realizadas	3 013 000	105 132 292 000	178 006 239 000	190 735 811 000
Saldo en curso de las tarjetas de prepago				

Entre 2012 y junio de 2016, los únicos bancos cameruneses que aceptaron comunicar información, gracias a la insistencia de la autoridad monetaria de Camerún pero también hay que decir que junto con amenazas de sanciones en caso de no colaboración, emitieron tarjetas bancarias de prepago por un valor global de transacciones de 868 401 600 301 FCFA (1 323 863 650 €). Además del hecho de que sus proyecciones según las cifras a 30 de junio de 2016 hacen prever una progresión de los valores de transacción equivalente al doble de las de 2015, dos de las instituciones bancarias no muestran ningún saldo en curso de las tarjetas de prepago de 31 de diciembre de cada año.

En la subregión, la ausencia de un dispositivo que dé una vista global del sistema de pago mediante tarjetas de prepago ha sido una desventaja bastante importante para recopilar datos. En efecto, no existe una entidad como en Portugal que gestione el conjunto de los cajeros automáticos. Por otra parte, no existe un referencial centralizador de las tarjetas que mencione los nombres de los usuarios y los números de las tarjetas, etc. De las entrevistas con los diferentes actores, se desprende que el control de los flujos de las operaciones con tarjetas de prepago no es un objetivo de las autoridades subregionales de regulación y de supervisión, que tienen entre sus misiones, hay que recordar, vigilar la estabilidad financiera y monetaria subregional.

2.1.2 El mobile money

Para la mayoría de las instituciones implicadas en la oferta de mobile money este medio de pago se introdujo en la Subregión después de 2010. Permite realizar transacciones gracias a un sistema de unidades monetarias a través del teléfono móvil. Las transacciones con mobile money están relacionadas con la apertura de una cuenta electrónica. La autorización para que un operador de telefonía móvil ofrezca un producto de mobile

money se obtiene a través de un banco colaborador que constituye un fondo de garantía para cubrir el volumen de dinero electrónico en circulación. Por lo tanto, los emisores de mobile money son bancos. En la CEMAC, se ofrecen los productos de mobile money siguientes:

Transferencias nacionales: transferencias de dinero entre dos personas residentes en el mismo país (también llamadas P2P).

Almacenamiento de dinero: en algunos sistemas, la cuenta sirve para almacenar dinero de forma segura, ya sea a través de una cuenta abierta en un banco o, de forma más habitual, en una cuenta abierta con el operador de móvil.

Pagos de compras al por menor: pago a los comercios participantes. Estos comercios pueden ser supermercados, distribuidores de bienes de consumo o el mismo operador de móvil (para la compra de crédito de tiempo de llamada u otros servicios por parte de los usuarios).

Pagos de facturas y otros servicios: para el pago de facturas de servicios de primera necesidad como el agua, la luz, que aportan comodidad y eficacia, para el pago de gastos escolares, impuestos...

Tabla 3: Lista de las entidades de crédito de la CEMAC autorizadas para emitir mobile money

País	Emisor	Operador técnico	Tipo de producto	Fecha de autorización
Camerún	BICEC	Orange	Mobile Money	29/07/2011
	ECOBANK	MTN	Mobile Money	29/07/2011
	Afriland First Bank	MTN	Mobile Money	29/07/2011
	SGC		Mobile Money	02/12/2011
TOTAL		4		
Congo	ECOBANK	MTN	Mobile Money	29/07/2011
	BGFI BANK	Airtel	Mobile Money	03/10/2011
TOTAL		2		
Gabón	BGFI BANK	Airtel	Mobile Money	29/07/2011
	BICIG		Mobile Money	11/07/2012
	ORABANK	Atlantique Télécoms (Moov)	Mobile Money	
	UGB	Gabon Telecom	Mobile Money	20/01/2014

TOTAL				4
Chad	ECOBANK	Airtel	Mobile Money	05/03/2012
	ORABANK	TIGO	Mobile Money	11/07/2012
TOTAL				2
TOTAL GLOBAL				12

Fuente: BEAC

Al leer esta tabla, podemos ver que de la cincuentena de bancos que ejercen en la subregión, solo doce de ellos poseen las autorizaciones para la emisión de mobile money. Entre los bancos que disponen de autorización, algunos como Soci t  G n rale o incluso Ecobank en Camer n siguen sin emitir mobile money.

2.4.2.1 La distribuci n de mobile money

Mobile Money es un servicio que permite que los clientes realicen transacciones financieras usando su tel fono m vil.

Este servicio es una herramienta importante para la inclusi n financiera. Permite introducir en el circuito bancario a una parte importante de la poblaci n que no usa servicios bancarios.

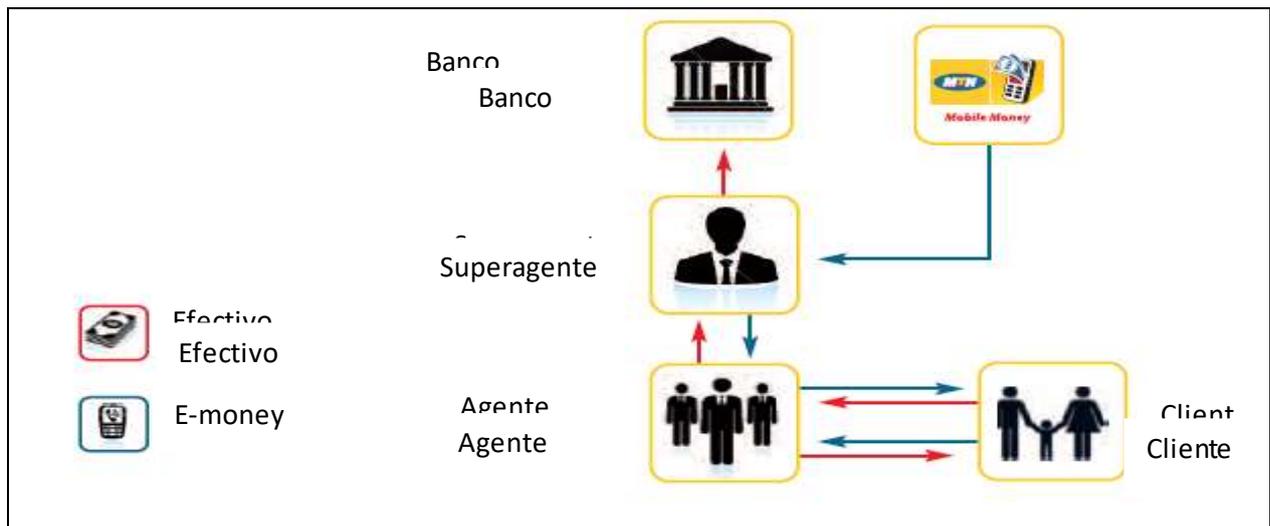
El Banco Central reglament  el Mobile Money poniendo en marcha una colaboraci n entre los bancos, que solo tienen autorizaci n de emitir moneda electr nica, y los operadores de telefon a m vil para que el servicio sea accesible a sus clientes.

El uso de mobile money implica a varios intervinientes:

- el banco, depositario de todos los fondos virtuales circulantes en la plataforma Mobile Money;
- el operador de telefon a m vil, responsable de desarrollar la red Mobile Money, entregar las SIM a los clientes y, en general, gestionar la plataforma Mobile Money;
- el agente mobile money, que obtiene dinero virtual depositando un equivalente de la tesorer a f sica en el banco;
- el comercio que recibe los pagos de los clientes mobile money;

- el cliente, usuario final que abona y carga las cuentas Mobile Money en la red de distribuidores y tiene la posibilidad de realizar transacciones Mobile Money.

El banco colaborador gestiona el dinero equivalente a las flotas virtuales que circulan en las cuentas «mobile money». Controla y garantiza la emisión de moneda electrónica, garantiza la conformidad de las operaciones con las leyes vigentes relativas al blanqueo de dinero y la financiación del terrorismo. Los bancos no siempre disponen de una plataforma. Se observa más bien a proveedores de servicio con plataformas multibanco.



El regulador no tiene acceso a las plataformas en tiempo real. Pero las plataformas están certificadas, lo que desde el punto de vista del regulador garantiza la fiabilidad de la gestión de las cuentas.

Sin embargo, los bancos tienen un acceso en tiempo real a la información de las plataformas. Las empresas de telefonía móvil gestionan la plataforma de las transacciones, incluida la flota virtual. Los distribuidores reciben la moneda creada y realizan la distribución. Realizan depósitos en la cuenta de garantía con fines de puesta a disposición de mobile money para los revendedores y agentes de distribución. Los agentes de distribución están vinculados a los distribuidores y realizan operaciones de retiradas y depósitos en las cuentas de los clientes. Los aceptadores son comercios que aceptan los pagos mediante mobile money.

Para abastecerse de mobile money, los distribuidores compran unidades de moneda electrónica a los operadores de telefonía móvil. Los revendedores recurren entonces a los distribuidores. Los clientes finales se abastecen ellos mismos de unidades de moneda electrónica entregando a cambio dinero en efectivo en los puntos de venta de los revendedores y de los minoristas.

Para que un comercio reciba pagos mediante mobile money, debe cumplir un conjunto de condiciones, formalizadas por la realización de un expediente jurídico que será estudiado por un agente de la compañía de telefonía móvil, y dado el caso, la firma de un contrato, previamente validado por un banco colaborador, entre él y el operador de telefonía móvil. Después se le abre una cuenta de comercio en la plataforma de gestión del operador de telefonía móvil y se remite una copia del contrato al banco para abrir la cuenta de comercio en la plataforma.

Para los distribuidores y los aceptadores, el expediente incluye la tarjeta de contribuyente, la inscripción en el registro mercantil, el plano de ubicación, una foto del gerente y justificantes de domicilio, como facturas de agua o luz. En la plataforma, el banco dispone de una lista de distribuidores y otros intermediarios, pero no de los clientes finales. Por lo tanto, no tiene rastro de las transacciones realizadas por los clientes finales. Controla más bien las existencias de moneda electrónica disponible.

La distribución de mobile money requiere la comunicación, por los operadores de telefonía móvil a sus bancos colaboradores, de una cierta cantidad de información. Concierno en especial los volúmenes de las transacciones, el fraude, las actividades de los distribuidores, el respeto de la reglamentación sobre los importes y los umbrales de las transacciones.

2.4.2.2 La demanda de mobile money en la CEMAC

Los usuarios de mobile money son principalmente personas físicas y jurídicas, que disponen o no de una cuenta bancaria, abonados de los operadores de telefonía móvil. Entre ellas, encontramos personas residentes

en las zonas periurbanas y rurales, comerciantes y empleados que no usan servicios bancarios.

El mobile money permite realizar reintegros en efectivo, así como pagos de facturas en los comercios, el pago de los impuestos y de las tasas, los pagos en línea, las compras de artículos, créditos de comunicación y transferencias de dinero. Se trata sobre todo de transferencias de dinero peer to peer (P2P)¹⁵, peer to cash (P2C). Además, el mobile money favorece la recolecta del ahorro de las poblaciones que no usan servicios bancarios o que residen en zonas rurales, contribuyendo de ese modo a la inclusión financiera. Para poder usar el mobile money, el cliente debe disponer de una línea telefónica y cumplimentar un formulario de suscripción adjuntando una copia de su documento nacional de identidad. La tabla siguiente presenta estadísticas sobre la actividad de mobile money en zona CEMAC; solo Airtel en Gabón, MTN y Orange (y sus bancos colaboradores respectivos Afriland First Bank y BICEC) en Camerún, aportaron información abundante.

Tal como se ilustra en las tablas siguientes y con base en la información recopilada de los únicos operadores de Camerún y Gabón, cerca de 868 702 238 000 FCFA (1 324 321 000 €) transitaron por el modo de pago mobile money entre 2011 y finales de junio de 2016.

Tablas 4 y 5: Oferta de Mobile Money en África Central (fuente: datos de investigaciones)
Estadísticas acerca de mobile money –MTN y Orange –Camerún

Indicadores	2011*	2012*	2013	2014	2015	2016 (a 30/06/2016)
Número de cuentas de moneda móvil registradas	42 996	628 378	2 738 901	3 589 086	3 796 051	6 284 061
Número de cuentas de moneda móvil activas	3589	68 799	1 442 692	1 738 976	2 172 792	2 808 249
Número de agentes registraos	659	264	6849	5991	17 219	11 952
Número de agentes activos	206	400	1969	4461	4943	6379
Valor de las transacciones bancarias móviles realizadas (en miles)	372 581	7 563 478	30 789 734	71 993 361	201 397 836	315 685 248
Número de transacciones bancarias móviles realizadas	35 475	998 277	3 273 148	8 951 175	25 096 057	28 907 949
Saldos en curso de las cuentas bancarias (en miles)	20 499	172 039	1 840 056	8 790 596	9 845 234	10 159 347

*estadísticas que solo conciernen al operador Orange Cameroun

¹⁵ Modelo de red informática donde cada cliente también es un servidor.

Indicadores	2012	2013	2014
Número de cuentas de mobile money	294 428	2 687 540	6 261 740
Valor de las transacciones	12 600 000	76 100 000	152 200 000

En la CEMAC y especialmente en Camerún, constatamos que el uso de mobile money empezó a extenderse a partir de 2013. En dicho año, el número de cuentas mobile money registradas con los operadores técnicos superó la barrera de los dos millones setecientos mil y las cuentas activas conocieron su progresión anual más elevada durante el periodo 2011 - finales de junio 2016, es decir cerca de un 2000 %. Tal como se esperaba, el número de agentes que participan en la distribución aumenta del mismo modo que las cuentas mobile money, con un pico en 2013.

En 2016, el número total de cuentas supera los seis millones docientos mil. Solo una cuenta de cada tres no está activa.

Tratándose de los flujos financieros movilizados a través de las transacciones por mobile money, su valor anual aumenta de media un 170 % cada año desde 2013. A finales de junio de 2016 (1.^{er} semestre), este valor se estima en más de 315 mil millones de FCFA (un 57 % más que el valor total del año anterior).

La ralentización del crecimiento de las existencias (de los saldos) en curso de las cuentas mobile money confirma la función principal de la transferencia de dinero «instantánea» que desempeña este instrumento entre sus usuarios y el aumento de la velocidad de la circulación de los flujos financieros movilizados. Por lo tanto, podemos observar que los saldos en curso de los bancos cameruneses, con respecto a esta herramienta, han progresado según una evolución anual del 970 % en 2013, pero solamente del 12 % en 2015 (incluso del 3 % en el primer semestre de 2016). Lo que quiere decir que las transferencias a través de mobile money se realizan con plazos cada vez más cortos.

En Gabón, el valor total de las transacciones mobile money del operador Airtel se duplicó en dos años y se sitúa en más de 150 mil millones de FCFA en 2014, y al igual que en Camerún, 2013 fue un año de transición con más del 813 % de aumento del número de cuentas de mobile money abiertas con AIRTEL GABON. En 2014, el número de cuentas se acerca a los seis millones trescientos mil.¹⁶

Resumiendo, basándose en los casos de las instituciones estudiadas, se puede decir que la demanda de mobile money en la zona CEMAC ha conocido un aumento muy fuerte durante los tres últimos años. Asimismo, el volumen de las transacciones a través de mobile money ha conocido una progresión fulgurante.

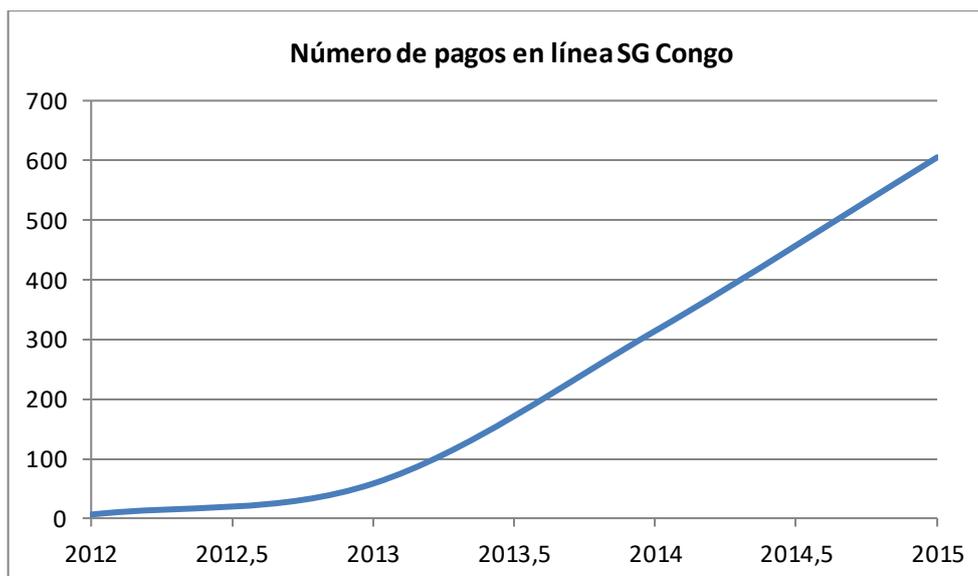
2.1.3 Los pagos en línea

Los pagos en línea comenzaron en la CEMAC a principio de los años 2000. Los principales actores que se lanzaron a la oferta de pago en línea fueron la pasarela de pago en línea, los sitios web y los bancos.

La pasarela de pago en línea representa un proveedor de productos de pago en línea. Para realizar una operación de pago en línea, se realiza la creación de un espacio asignado al cliente en la web donde se realizan las compras. Además, el proveedor de acceso a internet realiza una autenticación del espacio asignado al cliente cada vez que este intenta usar el sitio para realizar una compra.

En una estructura como Soci t  G n rale del Congo, el n mero de transacciones con pagos en l nea conoce efectivamente una evoluci n al alza de un a o para otro, aunque sigue siendo bajo: 605 pagos en l nea en 2015. Esta evoluci n se representa en el gr fico siguiente:

¹⁶ Con respecto a la poblaci n de Gab n (1 800 000 habitantes), el grupo de trabajo piensa que el n mero de cuentas presentadas procede de una falta de actualizaci n de los archivos de los clientes del operador implicado.



Para poder realizar pagos en línea, los clientes tienen la obligación de inscribirse en un sitio de comercio, suscribir un contrato, disponer de un identificador y una contraseña. Además, el cliente debe acceder a un espacio reservado para él y disponer de un monedero electrónico o de una tarjeta de afiliado a un sistema de pago internacional. Los pagos en línea conciernen principalmente compras de bienes y servicios, pero algunos bancos ofrecen un servicio de transferencias en línea. Los usuarios de pagos en línea son principalmente empresas y personas físicas que en su mayoría ya han estado en el extranjero.

La oferta de los NMP en la subregión plantea múltiples problemas que son a la vez técnicos, de control y de regulación. Los problemas técnicos son relativos a la inestabilidad de la red. Los problemas de control conciernen el bajo control del banco sobre las actividades de las ofertas de los NMP por sus colaboradores. La información sobre las actividades de los colaboradores de los bancos no siempre está completa o disponible en tiempo real. El control de la identidad de los usuarios, del origen de los fondos y de los umbrales reglamentarios no siempre se realiza. Por otra parte, la regulación y la supervisión de las autoridades monetarias sobre las actividades de oferta de los NMP no son efectivas.

Capítulo III

Los riesgos de blanqueo de dinero y de financiación del terrorismo a través de los nuevos medios de pago en la CEMAC

El auge de las Tecnologías de la Información y de la Comunicación (TIC) (principalmente de la telefonía) y la firme voluntad de los países de la subregión de reducir el fenómeno de exclusión financiera han favorecido el desarrollo y la expansión de la oferta de nuevos instrumentos de pago tales como las tarjetas de prepago y el mobile money. Aunque no se puedan rebatir las ventajas y los beneficios de este producto, su uso puede favorecer algunos comportamientos reprehensibles con respecto a las leyes y los reglamentos dictaminados por los Estados miembros de la CEMAC.

Sin embargo, el equipo de investigación ha identificado que los riesgos de blanqueo de dinero y de financiación del terrorismo a consecuencia del uso de los nuevos medios de pago están mal entendidos por los diferentes actores de la cadena que, a pesar de estar formados y sensibilizados sobre las diligencias a las que están obligados con respecto a su clientela en el momento de la ejecución de sus operaciones corrientes, no están avisados del uso fraudulento que podrían hacer malhechores de todo tipo.

El seminario organizado por el GABAC cuando se lanzó el presente ejercicio de tipologías y durante el cual varios especialistas procedentes de horizontes y profesiones diferentes del ámbito tuvieron que hacer presentaciones temáticas sobre los NMP y las entrevistas y sesiones de trabajo que el grupo de trabajo tuvo que organizar durante todo el ejercicio permitieron identificar algunas de las vulnerabilidades con respecto al blanqueo de dinero y la financiación del terrorismo inherentes al uso de los nuevos medios de pago en África Central.

Las costumbres de consumo en la subregión son tales que el comercio en línea de los productos está muy limitado. Solo presentaremos los riesgos o las vulnerabilidades con respecto al blanqueo de dinero y la financiación del

terrorismo relacionados con el uso de tarjetas de prepago y de mobile money.

3.1 Riesgos comunes a los nuevos medios de pago

3.1.1 Riesgos relativos a los fallos del dispositivo reglamentario

A pesar de su introducción relativamente reciente, la reglamentación sobre el funcionamiento de la actividad de emisión de moneda electrónica y el uso de los NMP parece tener en cuenta los posibles desvíos que pueden conducir al blanqueo de capitales y a la financiación del terrorismo. Sin embargo, todavía hay lagunas reglamentarias que podrían favorecer que se produjeran estos fenómenos. En efecto, el dispositivo que rige el uso de los NMP en la zona CEMAC presenta cierta vacuidad con respecto a los aspectos relativos a la lucha antiblanqueo de dinero y contra la financiación del terrorismo (Ndjimba, 2016), especialmente con los aspectos siguientes:

- la ausencia de un dispositivo reglamentario específico a los NMP y la regulación de los riesgos que su uso puede generar;
- el control sobre el origen de los fondos depositados a modo de contrapartida por la emisión de moneda electrónica, el objeto de las transacciones, así como el destino de los fondos. Disposiciones en este sentido ayudan a una mejor trazabilidad de las operaciones;
- el control de las transacciones en tiempo real con el objetivo de reducir los riesgos relacionados con el carácter rápido de la circulación de la moneda electrónica a través de los NMP;
- el nivel de los umbrales sobre los volúmenes de transacción que permanecen demasiado elevados y parecen haber sido fijados sin tener en cuenta el posible carácter fragmentario de estas operaciones y un recurso posible al smurfing. La supervisión de los nuevos actores del mercado, especialmente los intervinientes en el circuito de distribución del mobile money. En efecto, este último puede presentar numerosas vulnerabilidades relacionadas con la baja formación de los agentes o distribuidores, a menudo no profesionales del sector financiero, el funcionamiento de los NMP, así como los dispositivos y

otros mecanismos de lucha contra los riesgos de BC/FT relacionados con el uso de estos.

A estos fallos reglamentarios con respecto al uso de los NMP con fines de blanqueo o de financiación del terrorismo, se añaden los límites que se pueden reconducir a los factores de riesgo relativos a la conducción de la actividad de emisión de moneda electrónica, y de los NMP que la vehiculan.

3.1.2 Riesgos relacionados con la variedad de los actores y la rapidez de las evoluciones tecnológicas

El grupo de trabajo ha hecho suyo el desarrollo general¹⁷: los riesgos propios de la moneda electrónica proceden de los relacionados con los diferentes intervinientes en la emisión, la gestión y la distribución de los productos, así como de las evoluciones rápidas de la tecnología, que a menudo va por delante de la adaptación necesaria de los poderes públicos.

A modo de ejemplo, cinco categorías de actores intervienen en la *cadena de valor* de la tarjeta de prepago:

- El *emisor* de la tarjeta, autorizado por una autoridad de control, soporta la responsabilidad ante dicha autoridad. También es responsable del buen funcionamiento de la tarjeta con respecto a los usuarios. La tarjeta de prepago es el soporte de la moneda electrónica;
- La *red* (MASTERCARD, VISA, AMERICAN EXPRESS, JCB-CUP...) que gestiona las autorizaciones de las transacciones. La pertenencia de la tarjeta a una red permite que esta sea aceptada en los puntos de venta afiliados a dicha red;
- El *procesador* que gestiona los aspectos tecnológicos e informáticos de la tarjeta;
- El «*program manager*» que se encarga de todos los aspectos *no tecnológicos*: marketing, packaging, conformidad, logística, gestión práctica del producto, atención al cliente. Puede tratarse de bancos, actores de mercados especializados, oficinas de cambio, pequeñas empresas, etc.;

¹⁷ Fuente: Estudio de TRACFIN, monedas electrónicas, monedas virtuales y nuevos riesgos.

- El *distribuidor* que comercializa la tarjeta y está en contacto directo con los clientes (estancieros, marca de distribución, comercios de proximidad).

La red, el procesador y el emisor realizan la identificación de las operaciones. El emisor de la tarjeta también conserva en sus sistemas (servidores de autorización) los números de tarjetas con fines de búsqueda posterior. Estos tres operadores pueden distinguir las operaciones realizadas con una tarjeta de prepago de las realizadas con una tarjeta bancaria clásica. En efecto, cuando se emite la tarjeta, esta se asocia a un número BIN, es decir un número de identificación que lleva una clave que permite definir si se trata de una tarjeta de prepago, una tarjeta de empresa o una tarjeta individual. Resulta que aunque el emisor sea responsable jurídicamente de la vigilancia en materia de blanqueo, los elementos constitutivos para conocer al cliente solo pueden recopilarse a través del «program manager» y del distribuidor.

Por otra parte, los actores del sector de la moneda electrónica, al menos en lo que se refiere esencialmente a los distribuidores, proceden de una cultura no bancaria cuya pericia y experiencia («know how») en materia de conocimiento del cliente está más limitada que en el sector financiero tradicional.

En efecto, las redes de distribución de estos nuevos métodos de pago son a menudo de operadores no financieros, poco implicados en la lucha contra el blanqueo de capitales y financiación del terrorismo, incluso refractarios a la vigilancia que puede ser percibida como un freno costoso a la distribución de estos productos.

Otro factor aumenta el riesgo de fallo; el mercado está en pleno desarrollo y poco estabilizado. Por consecuencia, las entidades están compitiendo con fuerza las unas contra las otras y rivalizan en imaginación para aumentar su volumen de negocios.

Tratándose de los riesgos relacionados con las evoluciones tecnológicas, conviene destacar la recomendación 15 del GAFI que prevé: «*Los países y las instituciones financieras deberían identificar y evaluar los riesgos de*

blanqueo de capitales o de financiación del terrorismo que pueden resultar (a) del desarrollo de nuevos productos y de nuevas prácticas comerciales, incluidos nuevos mecanismos de distribución y (b) del uso de tecnologías nuevas o en curso de desarrollo relacionadas con nuevos productos o productos ya existentes. En el caso de las instituciones financieras, esta evaluación del riesgo debería producirse antes del lanzamiento de nuevos productos o de nuevas prácticas comerciales o antes del uso de tecnologías nuevas o en desarrollo. Las entidades financieras deberían adoptar las medidas oportunas para gestionar o reducir estos riesgos». Por consecuencia, los emisores de moneda electrónica que entran en el campo de las instituciones financieras deberían poder ofrecer productos y procedimientos de control que permitan reducir el riesgo. Sin embargo, esta obligación no se respeta debido al carácter especialmente competitivo de este sector.

[Hay constancia de que en África Central, no se ha tomado ninguna medida para evaluar los riesgos de blanqueo de dinero y de financiación del terrorismo relacionados con la oferta de nuevos medios de pago antes de su salida al mercado]. Pero, las evoluciones tecnológicas van en el sentido de transacciones cada vez más rápidas y a menudo más veloces que las de las redes más tradicionales, ya sea la rapidez de carga o de descarga de estos nuevos medios de pago, pero también en lo que se refiere a la distinción entre compra de tarjetas/creación de una cuenta y la posibilidad de carga posterior/de transferencia de fondos, etc. mediante simple envío de un SMS o un clic a través de internet. Por lo tanto, esta rapidez de los flujos complica considerablemente el control y puede impedir la incautación y la congelación de los fondos procedentes de delitos. La cadena de información es más compleja que en un circuito bancario clásico: para la misma operación financiera, el análisis del flujo requiere contactar con varios interlocutores, algunos de ellos fuera de la jurisdicción de la CEMAC. Por consecuencia, el proceso de investigación sufre ralentización.

3.2 Riesgos relacionados con las tarjetas de prepago

3.2.1 Opacidad de los bancos

Todas las entidades bancarias de la subregión fueron invitadas a participar en el ejercicio de tipologías objeto del presente informe. Sin embargo, solo los que representan a grandes grupos internacionales y un banco con capitales cameruneses aceptaron involucrarse. No obstante, por una parte, los implicados no ofrecen el servicio de tarjetas de prepago para los primeros y el valor de las transacciones del segundo solo representa el 1,72 % de la muestra estudiada, y por otra parte, se ha comunicado a los miembros del grupo de trabajo que las entidades de crédito que no aceptaron colaborar con el ejercicio estarían implicadas en investigaciones relativas a transferencias de fondos a gran escala con destino a países de África del oeste afectados por el terrorismo y al cambio manual a favor de personas implicadas por el blanqueo de dinero en los países donde están implantados. Y finalmente, aumentan los límites de carga de las tarjetas de prepago.

3.2.2 Anonimato de los portadores

Las tarjetas de prepago pueden ser nominativas o anónimas, según las opciones. Generalmente, la tarjeta se vende a una clientela ocasional¹⁸ que no se identifica sistemáticamente y que paga su compra o sus recargas en efectivo. La compra de la tarjeta puede hacerse en un establecimiento obligado¹⁹ o en un distribuidor de moneda electrónica²⁰.

Al compartirse las funciones de la tarjeta de forma universal, los portadores anónimos se beneficiarían en principio de los mismos servicios que los portadores identificados con regularidad. Sin embargo, sin identificación formal, la entidad obligada o el distribuidor no son capaces de determinar la identidad del portador y el origen de los fondos que sirven para la compra de la tarjeta y su carga. En otros términos, un cliente que posee dinero de origen dudoso o procedente de actividades ilícitas puede

¹⁸ «Persona física o jurídica que no tiene cuenta en la entidad obligada a la que se dirige», Reglamento COBAC R-2005/01 relativo a las diligencias de las entidades obligadas en materia de lucha contra el blanqueo de capitales y la financiación del terrorismo en África Central.

¹⁹ Entidad habilitada para emitir moneda electrónica.

²⁰ Entidad que ofrece al portador del instrumento electrónico, según la ejecución de un contrato firmado con una entidad obligada, un servicio de carga, de recarga o de recaudación de moneda electrónica.

perfectamente introducir el producto de su delito en el sistema financiero formal a través de una o varias tarjetas de prepago. Por lo tanto, el anonimato de la tarjeta es una brecha en la que los delincuentes y mafiosos de todo tipo podrían fácilmente encontrar cobijo.

3.2.3 No respeto de los límites prescritos por el Banco Central

Los límites de carga, retirada, pago, transferencia o por transacción, que dejan creer que la puesta a disposición de las tarjetas de prepago se ha desviado de su objetivo de inclusión financiera, pueden conllevar abusos de todo tipo con respecto a las estadísticas presentadas anteriormente.

Especialmente, cuando estos son muy amplios y susceptibles de beneficiar a portadores anónimos. Actualmente, los límites de carga pueden llegar a 10 millones de FCFA (15 245 €) al mes en Camerún²¹ y 25 millones de FCFA (38 115 €) semanales ofrecido por un banco de Gabón para las tarjetas de prepago. Se practican los mismos límites para los reintegros en los cajeros automáticos y los pagos.

A pesar de que estas entidades obligadas definen estos límites en el interior de varios segmentos, permanecen para la mayoría muy elevados. Sobre todo en el caso de las operaciones de retirada. Sin contar que, a falta de un dispositivo de centralización de la información acerca de las transacciones mediante tarjetas de prepago, un cliente titular o no de cuentas bancarias puede, al mismo tiempo que respeta los límites reglamentarios definidos por cada uno de ellos, evitar los límites y realizar recargas repetidas en tantos bancos como quiera en su país de residencia y en la subregión.

3.2.4 Riesgos de blanqueo de productos del fraude fiscal y aduanero

En la subregión, las tarjetas de prepago son mayoritariamente usadas por operadores en relación con el comercio internacional. Es decir, los importadores para quienes, hay que decir, que el civismo fiscal no es una preocupación principal. Para tal fin, como en lo que se refiere a las tarjetas de débito, las tarjetas de prepago les dan la facultad no solamente de evitar la reglamentación comunitaria en materia de cambio, sino también pormenorizar los valores declarados en aduana y por lo tanto, los derechos y

²¹ Vigilancia competitiva

tasas correspondientes. Al igual que la base imponible de los impuestos interiores que deben pagar. Los beneficios adquiridos de forma fraudulenta se invierten en diversos sectores (inmobiliario, proyecto agrícola de gran envergadura, distribución de productos petrolíferos...).

A pesar de que este aspecto no sea objeto del presente estudio, queremos atraer la atención de las autoridades monetarias sobre el hecho de que más allá de las pérdidas en ingresos presupuestarios que genera y el déficit del balance comercial en el que participa ampliamente, el uso de las tarjetas de prepago en el comercio exterior podría ser una de las causas inexplicadas, y no de las menos importantes, del descenso de la cobertura de cambio a nivel de la cuenta de operaciones, sin contar la pérdida de tasas que podrían percibirse de las comisiones cargadas por los bancos sobre las transacciones realizadas por sus clientes fuera de la zona FCFA.

3.2.5 Blanqueo evitando los umbrales de las declaraciones automáticas

La mayoría de los países de la subregión han suscrito actos reglamentarios que, bajo ciertas condiciones, obligan a las entidades financieras a declarar sistemáticamente a las células de información financiera cualquier operación de depósito en efectivo de 5 000 000 FCFA (aproximadamente 7625 €). En el marco de la primera etapa del blanqueo (inversión), algunos operadores podrían recargar sus tarjetas de prepago de forma repetida con importes cada vez inferiores a los límites de las declaraciones automáticas. Introduciendo de ese modo en el circuito financiero el dinero que podría proceder por ejemplo de la corrupción o de la malversación de fondos, de la venta de droga, de la venta ilícita de piedras y metales preciosos o de cualquier otro producto del crimen.

3.2.6 Los riesgos relacionados con la realización de las operaciones

El control de los flujos de banca electrónica representa el principal factor de riesgo relacionado con la realización de transacciones utilizando los NMP. En la Subregión, los bancos no tienen el control de sus plataformas de banca electrónica localizadas fuera de sus jurisdicciones de actividades. Esto puede fomentar la manipulación de la información relativa a las transacciones realizadas mediante tarjetas de prepago desde los

servicios del proveedor y favorecer la realización de operaciones dudosas. Por otra parte, la calidad de la conexión a internet puede favorecer la realización de operaciones sin que sean objeto de un análisis en tiempo real.

Y además, la insuficiencia o la falta de formación del personal de los bancos sobre los sistemas de información responsable de las tarjetas de prepago y sobre la reglamentación y las técnicas de blanqueo de dinero puede favorecer la realización de transacciones dudosas a causa de los errores humanos. Asimismo, en presencia de indicios de una operación de blanqueo de dinero o de financiación del terrorismo, un agente no formado o insuficientemente, sobre el tema no tendrá la capacidad de identificar el carácter dudoso de las operaciones y, por tanto, la declaración de sospecha por la legislación no se realizará, salvo que exista un sistema de supervisión centralizado, capaz de detectar las operaciones dudosas que no se detectaron en el primer nivel de vigilancia.

En este caso, se trata de un riesgo operativo elevado, sobre todo cuando los órganos de supervisión no realizan controles regulares de las operaciones. Este riesgo está reforzado por el hecho de que en estas instituciones no existe un dispositivo electrónico de alerta que identifique los indicios de sospecha de blanqueo de dinero y de financiación del terrorismo. El control de las transacciones con un sistema manual de chequeo de los indicios resulta muy limitado. Tal forma de actuar es propensa a los errores y la incapacidad de los agentes para detectar sistemáticamente indicios, a causa de la cantidad considerable de operaciones que analizar.

La ausencia de un dispositivo informático de análisis de los indicios puede representar un fallo del sistema de gestión de las transacciones para identificar las de naturaleza dudosa.

Frente a estos múltiples factores de riesgo, de orden organizativo y sistémico, es indispensable desarrollar un dispositivo sistémico de prevención de los riesgos de blanqueo y de financiación del terrorismo.

3.3 Riesgos relacionados con el pago mediante mobile money

Los servicios de dinero móvil se están actualmente desarrollando dentro de numerosos mercados del mundo. Pruebas tangibles indican que estos servicios mejoran el acceso a los servicios financieros formales en los países en vías de desarrollo.

Sin embargo, el desarrollo de estos servicios suscita el temor de que puedan utilizarse con fines de blanqueo de capitales y financiación del terrorismo (BC/FT). A pesar de que hasta ahora haya habido muy pocos casos de BC/FT, los sistemas de dinero móvil son susceptibles de ser utilizados con estos fines en un futuro (de la misma forma que otros servicios financieros formales están actualmente implicados)²².

3.3.1 Riesgos relativos a la conducción de actividades a través de mobile money

Los riesgos de blanqueo de dinero y de financiación del terrorismo vinculados a la ejecución de operaciones a través de mobile money recaen principalmente en los fallos de los sistemas de gestión de estos instrumentos por las instituciones financieras y sus colaboradores respectivos. Estos riesgos pueden clasificarse en dos grupos: los relacionados con la identificación de la clientela y los correspondientes a la realización de operaciones en cada eslabón de la cadena de actores.

3.3.2 Los riesgos relacionados con la identificación de la clientela

El riesgo de blanqueo de dinero y de financiación del terrorismo aumenta en la Subregión en la medida que las personas físicas pueden más fácilmente recurrir a documentos de identificación falsos. La ausencia de un dispositivo eficaz de comprobación de la autenticidad de documentos de identidad por parte de los operadores de telefonía móvil representa un gran límite a la prevención de estos riesgos, sobre todo cuando en varios operadores de telefonía móvil, el uso de mobile money es posible en cuanto se identifica al cliente y no después de la comprobación de la autenticidad de su documento de identidad. Incluso en estas estructuras a menudo se

²² El dinero móvil al servicio de las personas que no usan servicios bancarios (Maria solin, Andrew Zerzan).

presenta la copia de este documento y la comprobación de la autenticidad del documento de identidad original es entonces imposible de realizar. Además, las posibilidades que tienen los actores de pasar de un país a otro, con la ausencia de una base de datos subregional de identificación de las personas físicas, puede favorecer que se produzcan estos riesgos. Por lo tanto, la libre circulación de las personas en los países de la Subregión representaría un factor de riesgo.

3.3.3 Los riesgos de blanqueo de dinero y de financiación del terrorismo relacionados con la clientela

Este riesgo puede producirse con una transferencia clásica con un origen o un destino criminal (por ejemplo, financiación del terrorismo). A pesar de que para la suscripción se puedan usar justificantes reales, también se puede presentar falsa información. La etapa de depósito en cuenta también puede servir para reciclar fondos de origen fraudulento a través del uso de tarjetas bancarias o tarjetas de crédito robadas (lo que puede considerarse como un proceso de «inversión»). Las operaciones también pueden servir para transferir fondos entre cómplices o para transferirlos a otros países cuyas jurisdicciones tienen reglamentaciones en materia de LAB/CFT menos estrictas, donde los fondos pueden ser usados para financiar otras actividades criminales. Esto se acompaña entonces de la retirada de estos importes en efectivo para su uso o su transferencia a través de otros medios.

3.3.4 Riesgos relacionados con los comerciantes

Estas personas pueden recibir importes sustanciales de pagos y hacer que aparezcan como el producto legítimo de su actividad (pudiendo incluirse la integración de fondos). Los comerciantes pueden ser ellos mismos criminales que timan a su clientela o que sirven de fachada para el blanqueo del producto de actividades de sus cómplices, haciéndose pasar ellos mismos por clientes.

3.3.5 Riesgos relacionados con los agentes, intermediarios y colaboradores de la actividad al por menor

Se encuentran en una ubicación estratégica en el ciclo de pago de los servicios de dinero móvil: la carga de importes en efectivo, el punto de compra o de retirada, y también la venta de los teléfonos susceptibles de ser utilizados para las operaciones. Por lo tanto, estas personas tienen la posibilidad de falsificar sus registros, ignorar las sospechas que deberían señalarse o simplemente representar un punto débil que no ejerce su función con toda la vigilancia necesaria.

3.3.6 Riesgos a través de los pagos transfronterizos

Los pagos transfronterizos pueden servir para desplazar fondos de origen criminal de su jurisdicción de origen hacia otra jurisdicción en la que pueden servir para otras actividades criminales, ser extraídos o de nuevo desplazados hacia otra jurisdicción. Los movimientos de fondos transfronterizos hacen que las investigaciones de las autoridades sean más difíciles y permiten camuflar el objeto de la transferencia. Por consecuencia, representan una fuente adicional de riesgo.

Capítulo IV

Tipologías de los riesgos de blanqueo de dinero y de financiación del terrorismo relacionados con los nuevos medios de pago

La conjugación de los riesgos de blanqueo de dinero y de financiación del terrorismo, anteriormente evocados, ha favorecido la observación de varios casos tipológicos demostrados de blanqueo de dinero y de financiación del terrorismo a través del canal de los nuevos medios de pago. Después de haberlas presentado, se han emitido propuestas para reducir el riesgo de BC/FT.

Casos de blanqueo de dinero y de financiación del terrorismo a través de los nuevos medios de pago en la CEMAC

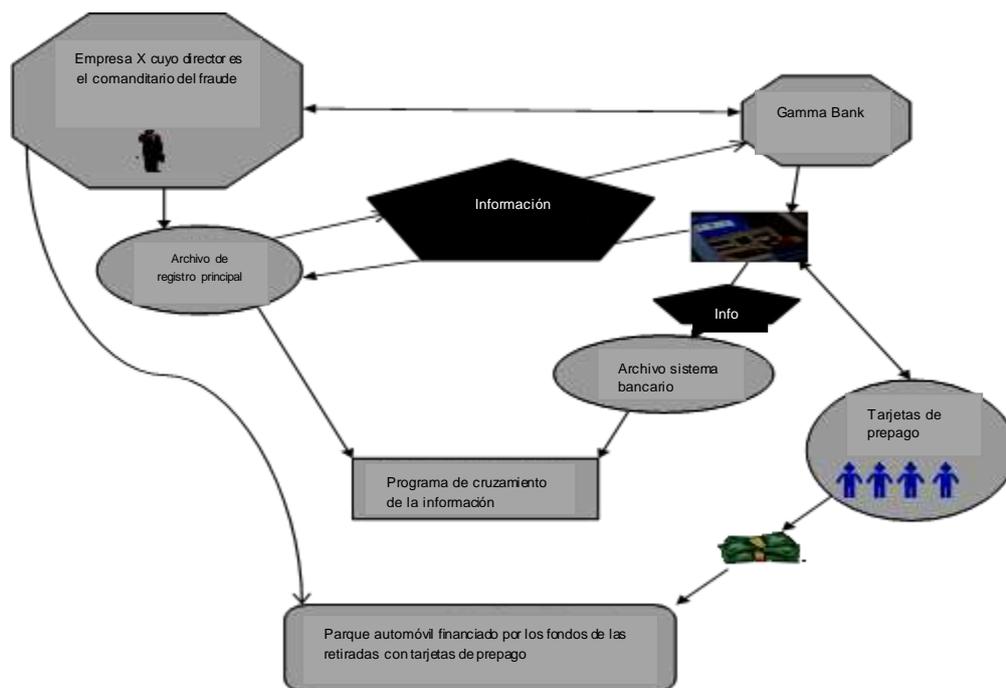
Con las investigaciones ante las ANIF, se han identificado dos casos tipológicos demostrados de blanqueo de dinero²³. El primer caso trata de un fraude informático con las tarjetas de prepago que permite un blanqueo de dinero.

²³ Se han identificado en el contexto francés casos tipológicos relativos al blanqueo de capitales mediante los NMP, altamente probables en la zona CEMAC con respecto a los factores de riesgo anteriormente identificados en el presente informe (informe T racfin 2011, casos 5 y 6, p. 18-23).

CASO 1: Fraude informático con tarjetas de prepago y blanqueo de dinero

La empresa X, especializada en soluciones de banca electrónica y cuyo director general era el denominado Pippo, era responsable de la gestión de la banca electrónica en Gamma Bank. Por ese motivo, alojaba y administraba los servidores de banca electrónica de Gamma Bank. El 12 de enero de 2015, el Sr. Pippo tuvo que responder ante los dirigentes de Gamma Bank porque al parecer se habían contabilizado operaciones en el sistema bancario, pero no en el sistema de banca electrónica. Una sesión de trabajo conjunta entre los informáticos de la empresa X y Gamma Bank reveló la existencia de retiradas en efectivo de los cajeros automáticos de Gamma Bank a través de 12 tarjetas magnéticas de prepago que pertenecían a 12 individuos. En efecto, estos 12 individuos poseían cada uno una tarjeta de crédito de prepago de Gamma Bank y realizaron varias retiradas de dinero en los cajeros automáticos. Después de cada operación, el jefe del departamento técnico de X, el Sr. Gando se conectaba al archivo de registro principal aumentando sus privilegios para modificar y borrar los rastros de las transacciones relacionadas con todas las actividades realizadas en un cajero automático en el que habían operado las 12 personas implicadas. Conociendo los plazos necesarios para las actualizaciones entre el sistema de banca electrónica y el sistema bancario, eliminaba la información relativa a las retiradas de dinero realizadas por sus comisionistas con las 12 tarjetas bancarias para impedir que el sistema bancario cargara en las cuentas implicadas el importe de dinero retirado. Una de las personas que realizaba retiradas repitió esta operación hasta el punto de expoliar a Gamma Bank 39 000 000 FCFA durante los años 2014 y 2015.

Sin embargo, Gamma Bank instaló una solución informática que realizaba, en un momento preciso, cruzamientos entre la información contenida en el archivo de registro del sistema bancario y la información contenida en el archivo de registro del sistema de banca electrónica. Dicha aplicación generó un informe de error que señaló la incapacidad de cruzar la información a causa de la eliminación de algunos datos en la tabla principal del sistema de banca electrónica. Después de analizar el informe de error, se constató que 12 cuentas «de crédito de prepago» no se cargaban con regularidad a pesar de las retiradas de dinero realizadas. Gamma Bank se dirigió entonces al director general de la empresa X, que abordó a su vez al denominado Alexander, basado en la India, proveedor y responsable técnico de la Zona África para la solución de banca electrónica que X distribuye en Camerún. Este último comprobó el sistema de banca electrónica de X y confirmó al señor Pippo que las operaciones de eliminación de la información de la tabla principal del sistema de banca electrónica se realizaron desde el interior de su empresa. Durante la investigación judicial, finalmente, el señor Gando reconoció los hechos antes de declarar un parque de venta de vehículos de segunda mano cuya actividad estaba financiada por el desvío de dinero.

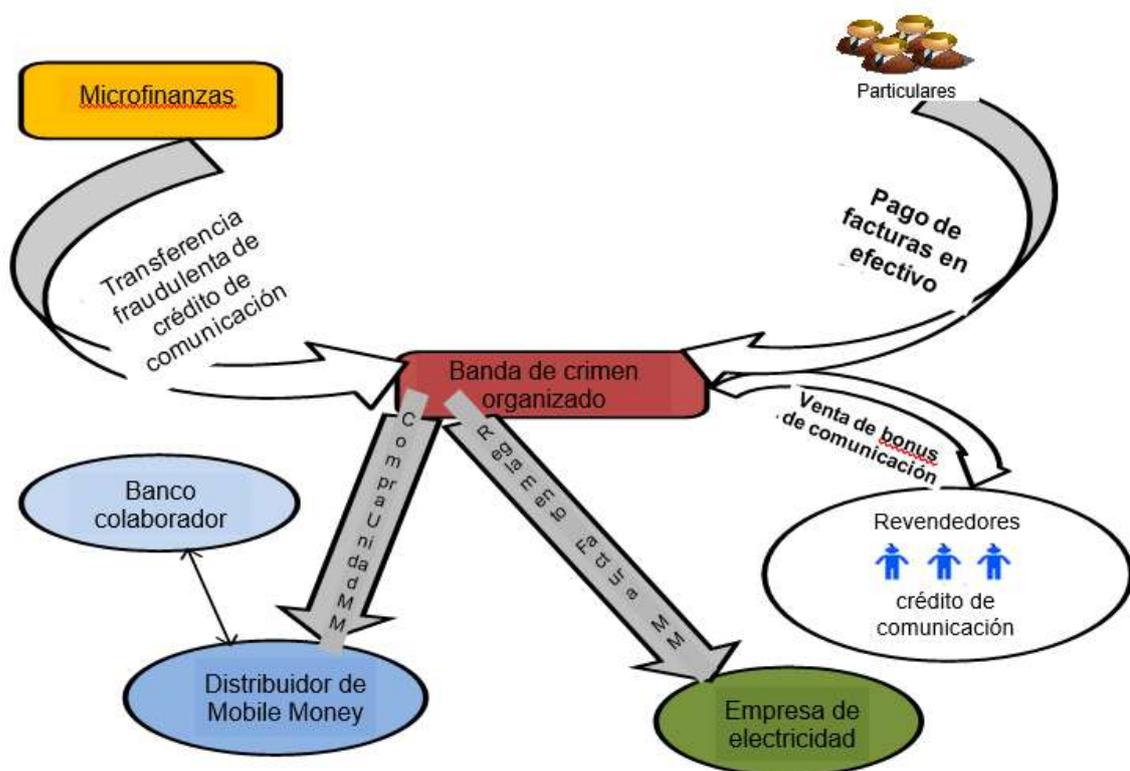


El segundo caso es relativo a una operación de blanqueo de dinero a través de mobile money.

Caso 2: Blanqueo de dinero a través de mobile money.

Después de haber sido condenada por estafa, la banda cuyo jefe se llama Ahomo se dio a conocer en prisión con otra forma de estafa. El 30 de mayo de 2014, el Sr. Bodo, empleado de una entidad de microfinanzas, puso en conocimiento del Ministerio Fiscal una denuncia por una estafa de la que había sido víctima. En efecto, sus verdugos imitaron la voz de su jefe para que realizara transferencias de crédito por valor de 900 000 FCFA. Después de la realización de las transferencias a números de teléfono específicos, los usurpadores cesaron cualquier comunicación con su víctima. La trazabilidad de las transacciones permitió establecer que estos créditos habían permitido el pago, mediante mobile money, de la factura de la luz de varias personas, servicio ofrecido por un operador de telefonía móvil del lugar. Después de la comparecencia y de la audiencia del señor Abondo, resultó que en su barrio en Bantoma, dos jóvenes que se hacían pasar por empleados de la compañía de electricidad habían ofrecido a la población la posibilidad de pagar sus facturas de la luz sin tener que hacer la cola en las agencias autorizadas.

Varios habitantes remitieron varias veces a estos falsos agentes, su recibo, el dinero en efectivo correspondiente al importe a pagar, así como los gastos de taxi. Indicó que después de cada operación, se les entregaba correctamente los recibos de pago de sus facturas. Además, después de cada pago de factura mediante mobile money, el operador de telefonía móvil otorgaba al abonado un bonus de créditos de llamada. Estos falsos agentes vendían entonces estos créditos a varios revendedores de crédito de comunicación, conocidos como «call boxeurs», a precios atractivos. Finalmente, el dinero percibido en efectivo de la población y de los call boxeurs se enviaba a la banda de Ahomo que seguía detenida en la prisión central



CAPÍTULO V

Recomendaciones para reducir los riesgos de blanqueo de dinero y de financiación del terrorismo relacionados con los nuevos medios de pago

Las recomendaciones para mejorar el dispositivo de gestión de los NMP en la subregión pueden consistir en propuestas relativas al control y la regulación de la actividad de oferta de estos instrumentos financieros y el sistema técnico de gestión de las transacciones a través de estos.

Estas propuestas conciernen principalmente:

- las mejoras del dispositivo reglamentario y de supervisión de la oferta de los NMP;
- la coordinación de las actividades entre los actores implicados en la gestión de esta actividad con la organización de sistemas para compartir automáticamente la información relativa a las transacciones que se realizan mediante moneda electrónica entre las empresas de emisión de forma que se facilite la recoleta de la información necesaria para las investigaciones, la detección de las operaciones sospechosas y sus declaraciones a las células de información financiera y los informes a las autoridades subregionales y nacionales de supervisión y de control;
- el refuerzo de las capacidades de los diferentes actores sobre el problema de blanqueo de dinero y financiación del terrorismo en general, pero sobre los riesgos de blanqueo de dinero y de financiación del terrorismo relacionados con esta rama de actividad.

5.1 Mejorar el dispositivo reglamentario de regulación y de supervisión de la actividad de oferta de los NMP

Los diferentes riesgos identificados en este informe, especialmente los relacionados con el anonimato de los portadores, los límites de las tarjetas de prepago, el blanqueo de productos del fraude fiscal y aduanero y la opacidad de los bancos de una parte y la dificultad de obtener estadísticas globales, a pesar de las disposiciones de la instrucción n.º GR/01 relativa a

la vigilancia por la BEAC de los sistemas de pago mediante moneda electrónica de otra parte, se deben esencialmente a carencias reglamentarias y a una falta de organización efectiva de la supervisión y de la vigilancia de las actividades relacionadas con los nuevos medios de pago por parte de las autoridades de regulación, de supervisión y de control tanto a nivel regional como a nivel nacional.

A parte que de forma general, en un entorno donde el pago de las transacciones se desmaterializa inexorablemente, estas carencias no permiten establecer de forma afinada los agregados de la masa monetaria y por lo tanto tomar las medidas adecuadas de estabilidad monetaria y financiera, tampoco permite una lucha antiblanqueo y contra la financiación del terrorismo eficaz.

Se han evocado anteriormente fallos reglamentarios. A estos, se debería añadir que a pesar de que, con respecto a los nuevos medios de pago, esclarecer las reglas antiblanqueo y contra la financiación del terrorismo dirigidas a las entidades de crédito incumbe a la COBAC como lo prevé la instrucción n.º GR/01, esta, hasta día de hoy, no ha puesto a disposición ninguna línea directora ni ningún otro acto que dictamine las diligencias propias a los nuevos medios de pago que los actores deberían aplicar en su relación con los colaboradores técnicos y la clientela.

En todo caso, pensamos que a falta de haber previamente aplicado la recomendación 15 del GAFI evocada anteriormente (véase punto 3-1-2), las autoridades competentes deberían mejorar la supervisión jurídica de los nuevos medios de pago para minimizar las vulnerabilidades con respecto al blanqueo de capitales y la financiación del terrorismo que les son inherentes.

El nuevo marco jurídico llevaría disposiciones que tienden a:

1. definir la función y las responsabilidades operativas de cada actor del desarrollo de las actividades de la moneda electrónica (autoridades de regulación, emisores, distribuidores...) consideradas individualmente y en sus relaciones de negocios;
2. enunciar las responsabilidades de los diferentes intervinientes en materia de lucha antiblanqueo y contra la financiación del terrorismo;

3. exigir la organización de un dispositivo técnico que disponga entre otras cosas de una pista de auditoría específica para garantizar la trazabilidad de las operaciones desde el origen de las órdenes de pago hasta su desenlace. Al facilitar su recolecta, la información contenida en dicha pista sería una fuente adicional para el enriquecimiento de las investigaciones después de las declaraciones de sospecha y, de forma más general, para las investigaciones llevadas a cabo por las autoridades de procedimientos;
4. Hacer respetar la reglamentación de los cambios de la subregión para las transacciones realizadas con la moneda electrónica en el marco del comercio exterior con países no miembros de la zona CEMAC;
5. Limitar los activos en moneda electrónica hasta un importe compatible con las políticas de inclusión financiera y los riesgos de blanqueo de dinero y de financiación del terrorismo que les son propios. Por ejemplo, en África del oeste, con reserva de una autorización especial del Banco Central, los activos en moneda electrónica no pueden superar los 2 000 000 FCFA (3000 € aproximadamente) al igual que cuando el portador dispone de varios instrumentos en una misma entidad, el cúmulo mensual de recarga no puede superar los 10 000 000 FCFA (15 250 € aproximadamente). A modo de ejemplo, el cúmulo semanal autorizado por un banco gabonés es de 25 000 000 (38 000 € aproximadamente). Todavía en África del oeste, el importe máximo en moneda electrónica que puede ponerse a disposición de un cliente no identificado es de 200 000 FCFA (305 € aproximadamente) durante un mismo mes;
6. Solicitar un informe sistemático y efectivo no solo a la BEAC sino también a las autoridades monetarias nacionales y autoridades aduaneras y fiscales (para las transacciones comerciales realizadas fuera de cada una de sus jurisdicciones respectivas), según una periodicidad y un esquema definido por la primera y cuyos datos podrán ser afinados en función de las peticiones de las autoridades responsables de las investigaciones;

7. Prever sanciones en caso de incumplimiento de las disposiciones reglamentarias;

En lo que se refiere especialmente al mobile money, las disposiciones de la reglamentación podrían contribuir a minimizar los riesgos identificados gracias a las medidas siguientes:

8. Para los riesgos relacionados con la clientela: cuando se trate de transacciones de persona a persona, desarrollar mecanismos destinados a identificar mejor a los emisores y los destinatarios de las transacciones electrónicas, instaurar límites sobre la cantidad de cuentas, la frecuencia de las operaciones, los volúmenes y los importes de transferencia que se pueden realizar durante un cierto periodo de tiempo; la vigilancia a nivel del sistema de los flujos de operaciones con el objetivo de señalar al proveedor de dinero móvil cualquier secuencia de operaciones sospechosa (de forma similar a los sistemas de LAB/CFT usados por los bancos y los sistemas de detección de fraudes usados por los operadores de telefonía móvil) los límites impuestos obligarían a los criminales y terroristas a fraccionar sus operaciones, lo que las haría más susceptibles de ser detectadas por el sistema;

9. Para los riesgos relacionados con los comerciantes: solicitar procedimientos de comprobación profundizados al inicio y durante la relación con el objetivo de reducir el riesgo hasta un nivel bajo;

10. Para los riesgos relacionados con los agentes, intermediarios y socios de la actividad al por menor: instaurar procedimientos de comprobación profundizados al inicio y durante la relación, así como una vigilancia continua del respeto de las obligaciones.

5.2. Coordinación de las actividades de los actores implicados en la gestión de los NMP

Independiente de las mejoras que se podrían aportar al marco jurídico relativo a los nuevos medios de pago, serían inoperantes en ausencia de instrumentos que permitan el control de su aplicación efectiva. Para ello, las

posibilidades que ofrecen las nuevas tecnologías de la información podrían ser de una utilidad más que apreciable.

Se trataría de instaurar un dispositivo que garantizara una mejor coordinación y un control riguroso de las actividades de los actores implicados en la oferta de los NMP con fines de lucha antiblanqueo y contra la financiación del terrorismo permitiendo que los actores tengan una vista sistemática de las transacciones financieras a través de los NMP en la CEMAC. Aseguraría también una centralización de la información (volumen, destino de los fondos, etc.) y una detección rápida de las operaciones de blanqueo de dinero y de financiación del terrorismo relacionadas con los NMP para permitir que las entidades de crédito, las autoridades de procedimientos autorizadas y la ANIF accedan y compartan la información relativa a los incidentes de pago declarados.

Tal dispositivo de naturaleza informática y telemática debería conectarse a los servidores, los cajeros automáticos, los TPE y las plataformas de banca electrónica de los diferentes actores que realizan la emisión de moneda electrónica en la subregión.

A modo de ejemplo, la instauración de límites puede resultar ineficaz si no existe interoperabilidad con respecto al uso de la moneda electrónica entre las plataformas de los emisores de la subregión. Plataformas dotadas con sistemas de bloqueo cada vez que hubiese un intento de superación del límite. Se podría imaginar el desarrollo de una solución técnica para compartir de forma instantánea información a través de un identificador único asignado a cada cliente y que estaría gestionado por un archivo central de los poseedores de moneda electrónica. Cualquier cosa que debiera ser una de las preocupaciones de la Agrupación Interbancaria de Banca Electrónica en África Central (GIMAC) en el marco del desarrollo de sus productos en particular, pero también en el marco de la ejecución de sus misiones estatutarias.

Para la lucha contra el blanqueo de dinero y la financiación del terrorismo, este dispositivo favorecería un seguimiento de los usuarios

sospechosos en la CEMAC. En efecto, podrá señalar los puntos de uso de los NMP y ayudar por tanto a reconstituir los itinerarios de los flujos de moneda electrónica, incluso de los criminales financieros. Al integrarle módulos de fraude y programas de detección de operaciones sospechosas (smurfing...), este dispositivo podría, mucho más rápidamente que los individuos, ayudar a iniciar declaraciones de sospecha de blanqueo de dinero y de financiación del terrorismo. Una operación fraudulenta que implicara a varios bancos y que desde el punto de vista de cada banco individual no dejara entrever nada anómalo, podría ser detectada desde un punto de vista global gracias a esta mecánica.

Sin embargo, su funcionamiento eficaz requeriría la implementación de las diferentes recomendaciones evocadas anteriormente. También sería necesaria la adhesión y la participación de los actores implicados en la oferta de los NMP y sobre todo la voluntad de los responsables políticos. Menos utópico de lo que se puede imaginar, la organización de tal dispositivo es factible y contribuiría fuertemente al control de los flujos monetarios relacionados con los NMP y la mitigación de los riesgos de blanqueo de dinero y de financiación del terrorismo asociados a su uso.

5.3 El refuerzo de las capacidades de los actores operativos

Una aplicación eficaz de las medidas de lucha antiblanqueo y contra la financiación supone no solamente un control de la reglamentación que la supervisa para abordar mejor el problema, sino también riesgos de desestabilización que el uso abusivo de los instrumentos de pago, especialmente los NMP, puede hacer correr a los sectores financieros, las economías y fragilizar la seguridad de los Estados.

Sería por lo tanto necesario una buena formación continua de los actores implicados por los NMP. Esta formación debe tratar el conocimiento del marco jurídico de la lucha antiblanqueo y contra la financiación del terrorismo y las técnicas de detección rápida de las operaciones atípicas asociadas a los nuevos medios de pago.

Para tal fin, la COBAC debería mediante líneas directoras (instrucciones), en conexión con el GABAC y/o las células de información financiera, indicar a los actores de la moneda electrónica las diligencias específicas a los nuevos medios de pago para protegerse de los riesgos de blanqueo de capitales y financiación del terrorismo y, además del Reglamento sobre prevención y represión del blanqueo de capitales, financiación del terrorismo y la proliferación en África Central de abril de 2016, para servir de soportes adicionales para el refuerzo de las capacidades de los diferentes actores de la cadena de los NMP.

Conclusión

En cumplimiento de estos términos de referencia, el objetivo de este ejercicio de tipologías era hacer un balance de los desarrollos de los NMP en la subregión, hacer un análisis comparativo de los diferentes enfoques reglamentarios susceptibles de regular y de supervisar el fenómeno de los NMP y mantener un equilibrio entre la necesidad de promover la inclusión de clases de poblaciones que no tienen acceso al sistema financiero y la lucha contra el blanqueo de dinero y la financiación del terrorismo; identificar los riesgos y las vulnerabilidades específicas inherentes a las tarjetas de prepago, a los sistemas de pago en línea (incluida la moneda virtual) y los servicios de pago a través de los teléfonos móviles, y finalmente, basándose en estudios de casos realizados al ser posible en la subregión, definir los modos operativos y las tendencias del uso abusivo de los NMP con fines de blanqueo de dinero y de financiación del terrorismo en África Central.

Con base en los datos recopilados, especialmente los flujos financieros que se desprenden, resulta del presente estudio que el volumen de las transacciones realizadas utilizando los NMP tal como se han definido anteriormente, conoce un fuerte aumento en la CEMAC, lo que demuestra que la franja de la población que de otra forma no hubiese podido acceder, ha optado por la oferta de los servicios financieros propuestos por los nuevos medios de pago. Especialmente el mobile money.

Sin embargo, una cierta cantidad de vulnerabilidades con respecto al blanqueo de dinero y financiación del terrorismo podría proceder de los nuevos medios de pago.

Se trata de las vulnerabilidades relacionadas con:

- La carencia del dispositivo reglamentario, la variedad de los actores y la rapidez de las evoluciones tecnológicas, para las comunes a los NMP estudiados;

- La opacidad de los bancos; el anonimato de los portadores: el no respeto de los límites recomendados por el Banco Central; el blanqueo de los productos del fraude fiscal y aduanero, la elusión de los umbrales de declaración automáticos y la realización de operaciones con respecto a las tarjetas de prepago.
- La clientela; la identificación de la clientela; los comerciantes; los agentes, intermediarios y socios de la actividad al por menor y los pagos transfronterizos con respecto al mobile money.

Se identificaron dos casos demostrados de blanqueo de dinero y de financiación del terrorismo relacionados con el uso de los NMP en la CEMAC: el primer caso trataba de un fraude informático con tarjetas de prepago que condujo a blanqueo de dinero y el segundo caso era relativo a una operación de blanqueo de dinero a través de mobile money.

Estos diferentes casos tipológicos se producen después, tal como se ha indicado anteriormente, de la conjugación de varios factores de riesgo de blanqueo de dinero y de financiación del terrorismo. Entre estos factores de riesgo, se pueden identificar los relativos a los fallos del dispositivo reglamentario. Se trata principalmente de una vacuidad del marco jurídico de los NMP a la hora de tratar aspectos relacionados con el blanqueo de dinero y la financiación del terrorismo, una ausencia de textos sobre el origen de los fondos, la identidad de los usuarios... y el control asociado a la conducción de actividades por mediación de los nuevos medios de pago y los límites de transacciones, que son demasiado elevados. También se identifican factores de riesgo relacionados con la alimentación de los nuevos medios de pago y la realización de las operaciones.

Para corregir estos factores de riesgo de tal forma que se frenen los riesgos de blanqueo de dinero y de financiación del terrorismo, se define un conjunto de recomendaciones. Estas recomendaciones conciernen el refuerzo del dispositivo reglamentario que supervisa la oferta de los NMP, con la propuesta de mecanismos que aseguren una mejor coordinación de las actividades de los actores implicados en la oferta de los NMP, el

desarrollo de un dispositivo de recolecta de la información en tiempo real de las transacciones a través de los NMP. La aplicación de esta batería de propuestas evoluciona gracias a una voluntad política y la participación concertada de los diferentes actores del sistema financiero puede fuertemente contribuir a un mejor control de las transacciones a través de los NMP y prevenir los riesgos de blanqueo de capitales y de financiación del terrorismo relacionados con su uso.

Lista de las siglas usadas en el informe

ANIF: Agencia Nacional de Investigación Financiera

BC: Blanqueo de capitales

BEAC: Banco de los Estados de África Central

BICEC: Banco Internacional de Camerún para el Ahorro y el Crédito

CEMAC: Comunidad Económica y Monetaria de los Estados de África Central

COBAC: Comisión Bancaria de África Central

EME: Entidad de Moneda Electrónica

FT: Financiación del Terrorismo

GABAC: Grupo de Acción contra el Blanqueo de Dinero en África Central

GIMAC: Agrupación Interbancaria de Banca Electrónica en África Central

LAB/FT: Lucha Antiblanqueo y contra la Financiación del Terrorismo

NMP: Nuevos Medios de Pago

UMAC: Unión Monetaria de África Central

Bibliografía

- 1- Adrianaivo, M, Kpodar, K, 2012, Mobile phones, financial inclusion and growth, Review of Economics and Institutions, Vol 3, No2 ;
- 2- Armendariz de Aghion, B., Morduch, J., 2005, “The economics of microfinance”, The Mit Press Cambridge, Massachusetts London.
- 3- L’argent mobile au service des personnes non bancarisées (Maria Solin, Andrew Zerzan)
- 4- Attali, J., 2006, “La microfinance aujourd’hui”, Planetfinance , télécharger à www.pointsdactu.org/article_print.php3?id_article=664.
- 5- Babajide, A, 2015, Financial inclusion and economic growth in Nigeria, International Journal of Economics and Financial Issues, Vol 5, No3,
- 6- CENAFE, 2010, Typologies et tendances en matière de blanchiment d’argent et de financement du terrorisme au sein des entreprises de services monétaires canadiennes - Rapport de typologies et de tendances de CENAFE.
- 7- CGAP, 2001, Commercialisation et dérive de la mission des IMF, la transformation de la microfinance en Amérique Latine, Etude Spéciale.
- 8- Chatain, P-L ., Hernandez-Coss, R., Borowik, K., Zerzan., 2008, Integrity in mobile phone financial services : Measures for mitigating risks from money laundering and terrorist financing, World Bank Working - Paper No 146.
- 9- Demetis, D., 2010, Technology and anti-money laundering : A systems theory and risks-based approach, Edgard Egar Publishing Limited.
- 10- Di Castri, S, Mobile money: Enabling regulatory solutions, www.gsma.com/.../2013/.../MMU-Enabling-Regulato..
- 11- Donovan, K, 2012, Mobile money for financial inclusion, siteresources.worldbank.org/.../IC4D-2012-Chapter-4.
- 12- Helms, B., 2006, “La finance pour tous: construire des systèmes financiers inclusifs”, Les éditions Saint-Martin.

- 13- Hulme, D., Mosley, P., 1996, "Finance against poverty", Volume 1, Routledge, London.
- 14- Investir au Cameroun, 2005, le Mobile money prend ses marques au Cameroun, N°38
- 15- Klein, M, Mayer, C, 2011, Mobile money and financial inclusion: The regulatory lessons, Policy research working paper 5664, World Bank.
- 16- Lal, R, Sachdev, I, 2015, Mobile money services, design and development for financial inclusion, Harvard Business School, Working paper 15-83
- 17- Lawack, V, 2013, Mobile money, financial inclusion and financial integrity : The South African Case, Washington Journal of Law, Technology and Art, Vol 8, No 3, p 317-346.
- 18- Lelart, M., 2002, L'évolution de la finance informelle et ses conséquences sur l'évolution des systèmes financiers, Réseau Entrepreneuriat, Cotonou 16-18 Avril.
- 19- Lelart, M., 2005, "De la finance informelle à la microfinance", Editions des Archives Contemporaines, AUF.
- 20- Levine, R, 2003, More on finance and growth : More finance, more growth ?, Federal Reserve Bank of St Louis Review, Vol 84, No 4, P31-46.
- 21- Mayoukou, C, 2000, La microfinance en Afrique centrale : Etat des lieux et perspectives de développement, TFD, 59-60, Juillet
- 22- Etude de TRACFIN, monnaie électronique, monnaies virtuelles et nouveaux risques.
- 23- Maria solin, Andrew Zerzan, L'argent mobile au service des personnes non bancarisées-2009

Lista de los textos reglamentarios relativos a la moneda electrónica

1. Reglamento n.º 01/02/CEMAC/UMAC/COBAC de 13 de abril de 2002 relativo a las condiciones de ejercicio y de control de la actividad de microfinanzas en los Estados de la CEMAC;
2. Reglamento n.º 01/03/CEMAC/UMAC de 4 de abril de 2003 sobre la prevención y represión del blanqueo de capitales y la financiación del terrorismo en África Central.
3. Reglamento n.º 02/03/CEMAC/UMAC/CM de 4 de abril de 2003 relativo a los sistemas, medios e incidentes de pago.
4. Reglamento n.º 01/11/CEMAC/UMAC/CM de 18 de septiembre de 2011 relativo al ejercicio de la actividad de emisión de moneda electrónica.
5. Reglamento de la COBAC R-2005/01 de 1 de abril de 2005 relativo a las diligencias de las entidades con obligaciones en materia de lucha contra el blanqueo de capitales y la financiación del terrorismo en África Central.
6. Reglamento de la COBAC R-2005/02 relativo a las entidades de moneda electrónica.
7. Instrucción de la COBAC I-2006/01 de 31 de julio de 2006 relativa a la información acerca del dispositivo de prevención del blanqueo de capitales y financiación del terrorismo.
8. Instrucción n.º 01/GR de 31 de octubre de 2011 del Gobernador de la BEAC, relativa a la vigilancia de los sistemas de pago mediante moneda electrónica, con en anexo un marco de referencias que recopila los elementos que permiten a la BEAC garantizar su misión de vigilancia de la actividad.
9. Instrucción n.º 02/GR/UMAC de 7 de mayo de 2014 del Gobernador de la BEAC, relativa a la puesta en marcha del multibanking en el marco de la actividad de emisión de moneda electrónica.

CONSULTA JURÍDICA

De

***Don Kévin Ferdinand Ndjimba, doctor en Derecho, docente e
investigador en la Universidad Omar Bongo, Libreville***

Relativa a

**ANÁLISIS COMPARADO DE LOS MARCOS JURÍDICOS DE LA CEDEAO Y DE LA CEMAC
RELATIVOS A LOS NUEVOS MEDIOS DE PAGO**

Libreville en Gabón, a 23 de abril de 2016

1. Mediante carta de la Secretaría Permanente del GABAC con fecha de 12 de abril de 2016, se solicitó mi pericia para analizar los marcos jurídicos de la Comunidad Económica de los Estados de África del Oeste (CEDEAO) y de la Comunidad Económica y Monetaria de África Central (CEMAC) relativos a los nuevos medios de pago.

2. Los documentos objeto de análisis son los siguientes:

- la Instrucción n.º 008-05-2015 que rige las condiciones y modalidades de ejercicio de las actividades de los emisores de moneda electrónica en los Estados miembros de la Unión Monetaria del Oeste Africano (UMOA) de 21 de mayo de 2015;

- El Reglamento n.º 01/11-CEMAC/UMAC/CM relativo al ejercicio de la actividad de emisión de moneda electrónica de 18 de septiembre de 2011.

- La Instrucción n.º 02/GR/UMAC relativa a la puesta en marcha del multibanking en el marco de la emisión de moneda electrónica de 7 de octubre de 2014;

- La Instrucción n.º 01/GR relativa a la vigilancia por parte de la BEAC de los sistemas de pago mediante moneda electrónica.

3. Después de haber examinado estos documentos y con respecto a los elementos contenidos en su carta mencionada anteriormente, resulta que su solicitud trata cuatro cuestiones esenciales:

- 1- ¿Cuál es la extensión del marco jurídico del uso de los medios de pago con respecto a las dos legislaciones comunitarias?
- 2- ¿Qué apreciaciones se pueden hacer de la legislación comunitaria CEMAC con respecto a la legislación comunitaria CEDEAO que pueda parecer más exitosa?
- 3- ¿En qué medida la supervisión jurídica ofrecida por la legislación CEMAC es susceptible de permitir luchar eficazmente contra el blanqueo de capitales y la financiación del terrorismo con estos nuevos medios de pago?
- 4- ¿Qué disposiciones tomar para una mejor prevención y un control más eficaz del eventual uso de estos nuevos medios de pago con el objetivo del blanqueo de capitales y la financiación del terrorismo en la subregión?

Por lo tanto, basándome en estas diferentes cuestiones, formularé las observaciones siguientes, tratando de responder de forma precisa a sus preocupaciones,

I- La supervisión jurídica del uso de nuevos medios de pago en la zona CEDEAO y en la zona CEMAC

4. Con un volumen desigual, las legislaciones CEDEAO y CEMAC con respecto al uso de los nuevos medios de pago, tienen de forma global la misma estrategia, por lo que a primera vista, parecen muy cercanas la una de la otra.

A- El marco jurídico CEDEAO

1- Presentación

5. En la CEDEAO, el marco jurídico relativo al uso de los nuevos medios de pago está contenido en la Instrucción n.º 008-05-2015 del Banco Central de los Estados de África del Oeste que rige las condiciones y modalidades de ejercicio de las actividades de los emisores de moneda electrónica en los Estados miembros de la UEMOA.

6. Se trata de un documento de una sesentena de páginas que se compone de una decisión del Gobernador del BCEAO de cuarenta y dos (42) artículos y de cinco (5) anexos que tratan especialmente:

- la lista de los documentos y la información que componen el expediente de solicitud de autorización en calidad de entidad de moneda electrónica (anexo 1);
- la lista de los documentos y la información que componen el expediente de creación de filiales o sucursales de una entidad de moneda electrónica (anexo 2);
- el esquema para la presentación de un expediente de solicitud de autorización en calidad de creación de moneda electrónica y del expediente de autorización del ejercicio de actividades de moneda electrónica (anexo 3);
- la exigencia de informe mensual (anexo 4);
- la exigencia de informe trimestral (anexo 5).

7. La Decisión del Gobernador que contiene lo esencial de las reglas de supervisión se divide en los siete (7) títulos siguientes:

Título I: Disposiciones generales;

Título II: Condiciones de otorgamiento de la Aprobación o de la Autorización de ejercer actividades de emisión de moneda electrónica;

Título III: Modalidades y condiciones generales de ejercicio de las actividades de emisión de moneda electrónica,

Título IV: Modalidades y condiciones específicas aplicables a las entidades de moneda electrónica;

Título V: Disposiciones relativas a la protección de los poseedores de moneda electrónica;

Título VI: Suspensión, control y sanciones

Título VII: Disposiciones transitorias.

2- Análisis

8. Tras leer todo el dispositivo jurídico de la CEDEAO, aparece que este tiene es exhaustivo, ya que su objeto se extiende a diversos actores que usan la moneda electrónica y prevé de forma más o menos precisa las diferentes obligaciones que se imponen a estos.

9. Más allá de las reglas y de las exigencias tradicionales relacionadas con las condiciones de obtención de la aprobación o de la autorización de ejercer las actividades relacionadas con la emisión de moneda electrónica, que de hecho son más o menos detalladas, la legislación comunitaria CEDEAO impone reglas precisas sobre algunos aspectos que permiten un mejor control y un mejor seguimiento de estas actividades en el marco de la lucha contra el blanqueo de capitales y la financiación del terrorismo.

Entre estas reglas podemos especialmente mencionar:

- la obligación para el beneficiario de la autorización de probar la existencia de una pista de auditoría que permita garantizar una trazabilidad de las operaciones desde el origen de la orden de pago hasta su desenlace;
- la instauración de una obligación de trazabilidad establecida durante un periodo de diez (10) años y que se impone no solamente a los emisores de moneda electrónica sino también a sus distribuidores que de hecho se responsabilizan de su actividad;
- la obligación para los emisores de moneda electrónica de vigilar que sus distribuidores principales y subdistribuidores apliquen las recomendaciones en materia de seguridad y vigilancia, definidas en el marco de su relación comercial, incluidas las medidas relativas a la lucha contra el blanqueo de capitales y financiación del terrorismo (**artículo 18**).

10. Además y tratándose principalmente de entidades de moneda electrónica, **la Instrucción especifica claramente su sumisión a la reglamentación vigente en materia de lucha contra el blanqueo de capitales y la financiación del terrorismo (artículo 26)**.

11. Con estos objetivos, se recomienda encarecidamente que estos:

- pongan en marcha un sistema automatizado de vigilancia de las transacciones que tienen como soporte la moneda electrónica (**artículo 26**);
- instaurar un dispositivo específico de lucha contra el blanqueo de capitales y la financiación del terrorismo (**artículo 26**);
- conservar todos los datos relativos a las operaciones que procesan durante un periodo de diez años contados desde el ejercicio durante el cual se han realizado estas transacciones;
- informar obligatoriamente a la CENTIF sobre las operaciones sospechosas.

Finalmente, el dispositivo jurídico prevé un conjunto de sanciones relacionadas con el incumplimiento de la reglamentación. Se trata especialmente:

- de sanciones financieras establecidas en forma de penalizaciones relacionadas con la no comunicación de la información a las autoridades de supervisión que son la BCEAO, la Comisión Bancaria de la UMOA y el Ministro responsable de finanzas de cada país;
- de la suspensión parcial o total de las actividades;
- de la retirada de la aprobación o autorización de emitir moneda electrónica.

12. De forma más general, se tiene que destacar que el dispositivo CEDEAO tiene en cuenta todas las categorías de emisores de moneda electrónica precisando tanto las obligaciones respectivas como las reglas fundamentales de su colaboración.

13. Al prever un dispositivo de control muy amplio y al precisar la extensión de ese control, la Instrucción de la BCEAO insta un marco jurídico que, a pesar de ser perfectible, somete la actividad de emisión de moneda electrónica a un control más o menos estrecho que garantiza la fluidez del sistema y la lucha contra su uso con fines criminales.

B- El marco jurídico CEMAC

14. El marco jurídico que reglamenta el ejercicio de la actividad de emisión de moneda electrónica en el espacio CEMAC está regido por el **Reglamento n.º 01/11 CEMAC/UMAC/CM de 18 de septiembre de 2011** y, en menor medida, por **la Instrucción n.º 02/GR/UMAC de 7 de mayo de 2014**.

15. El Reglamento n.º 01/11 CEMAC/UMAC/CM es un texto de treinta y siete (37) artículos agrupados en siete (7) capítulos relativos a:

- definiciones (capítulo 1);
- el objeto y el campo de aplicación (capítulo 2);
- las condiciones de ejercicio de la actividad de emisión de moneda electrónica (capítulo 3);
- el régimen de emisión de moneda electrónica y su conversión en moneda fiduciaria o escritural (capítulo 4);
- la regulación del control y la vigilancia de la actividad de emisión de moneda electrónica (capítulo 5);
- el cese de la actividad de emisión de moneda electrónica (capítulo 6);
- las disposiciones transitorias y finales (capítulo 7).

16. De forma global, este texto define las reglas generales aplicables a esta actividad.

De ese modo, atribuye la exclusividad del ejercicio de la actividad de emisión de moneda electrónica solamente a las entidades de crédito. Dicho ejercicio está condicionado por la obtención de una autorización entregada por el

Gobernador de la BEAC tras un informe de un Comité Técnico que se compone de expertos de la BEAC, de la Secretaría General de la COBAC y del órgano responsable de la regulación de la actividad de banca electrónica en la CEMAC.

Someter la obtención de esta autorización a la presentación de una cierta cantidad de documentos directamente listados en el artículo 5 y entre los cuales los más importantes son:

- los documentos que definen las cualidades y poderes de los representantes legales;
- la descripción detallada de las relaciones de participación en capital entre las diferentes personas que intervienen en el proceso de emisión de moneda electrónica;
- las copias de los proyectos de convenios a establecer con el resto de actores de la actividad tales como socios técnicos o financieros, los vendedores o distribuidores, los comerciantes o aceptadores y los suscriptores de la moneda electrónica;
- otros elementos técnicos que permiten establecer la fiabilidad del sistema.

17. Por otro lado, el Reglamento determina el contenido de los contratos celebrados entre los establecimientos emisores y los portadores, los aceptadores. Estos deben contener la lista de las entidades que pertenecen a la red y los límites relativos a la carga o descarga de la moneda electrónica, al pago y transferencia de unidad de valor de cuenta a cuenta y la tarificación de los servicios.

Prevé además una trazabilidad de las transacciones electrónicas durante tres (3) años, pero también diversas disposiciones relativas especialmente a la garantía de la existencia de fondos y la fluidez de las operaciones.

18. En materia de regulación, de control y de vigilancia de la actividad, el reglamento da competencia a la BEAC y al COBAC.

La primera se encarga de fijar las normas jurídicas de emisión de moneda electrónica y de su conversión en moneda fiduciaria o escritural y las normas técnicas aplicables a los sistemas de puesta en marcha para garantizar la seguridad, la eficacia y la credibilidad de la moneda electrónica. También tiene la competencia de vigilancia, organizando un referencial de vigilancia.

La segunda tiene competencia para fijar las normas de prudencia que deben respetar los establecimientos para la garantía de fondos, las normas de lucha contra el blanqueo de capitales y la financiación del terrorismo, las normas de trazabilidad contable, las reglas relativas al capital mínimo de las EMT y la cotación SYSCO. También tiene competencia para ejercer el control de las entidades.

19. Para el ejercicio del conjunto de estas misiones, el Reglamento atribuye a las entidades una obligación de información y notificación y en beneficio de estas dos instancias, un derecho de acceso lo más amplio posible a

cualquier información, reforzado por la no oponibilidad del secreto profesional.

20. El control que ejercen también se extiende a los socios técnicos y a los socios comerciales. Sin embargo, el control ejercido sobre los socios técnicos solo tiene en cuenta los aspectos técnicos, mientras que el de los socios comerciales tiene el objetivo de comprobar la aplicación efectiva del régimen.

El resultado de estos dos controles puede saldarse con:

- la notificación de recomendación de puesta en conformidad;
- la orden de aplicar las recomendaciones;
- el aviso o la aplicación de las sanciones previstas por la ley.

21. Finalmente, el reglamento precisa las condiciones de cese de la actividad de emisión de moneda electrónica, que son:

- la solicitud de la entidad implicada;
- la toma de posesión de la COBAC;
- la ausencia de uso de su autorización en un plazo de doce (12) meses o la inactividad durante 6 meses;
- la falta posterior a las condiciones de la autorización.

22. La **Instrucción n.º 02/GR/UMAC** es un texto de 48 artículos agrupados en nueve (9) capítulos que tratan respectivamente:

- las definiciones;
- el objeto;
- las condiciones y modalidades de participación en el multibanking;
- el funcionamiento de la red de multibanking;
- la compensación y el reglamento entre los participantes de una red de multibanking;
- los fondos de garantía de la red de multibanking;
- la vigilancia del multibanking;
- las disposiciones transitorias.

23. El objeto esencial de esta instrucción es aplicar las reglas que rigen el dispositivo que permite a los emisores de moneda electrónica, que tienen en común el mismo gestor técnico, constituirse en red interoperable en una plataforma técnica única, no aporta ningún elemento pertinente con respecto al riesgo que puede representar esta actividad en materia de blanqueo de capitales y de financiación del terrorismo.

Por ejemplo, en materia de vigilancia, la Instrucción solo aborda cuestiones relativas a la compensación y los incidentes técnicos.

24. La **instrucción n.º 01/GR relativa a la vigilancia por parte de la BEAC de los sistemas de moneda electrónica** es un texto de 15 artículos agrupados en cuatro (4) capítulos dedicados respectivamente a:

- las definiciones y el objeto de la Instrucción;
- la organización de la vigilancia de las entidades obligadas;
- las modalidades de puesta en marcha de la vigilancia de las entidades obligadas;

- las disposiciones transitorias y finales.

25. Esta instrucción, adoptada en cumplimiento de las prescripciones del Reglamento n.º 01/11 CEMAC/UMAC/CM, trata esencialmente de las reglas de procedimiento relativas al control. Define, como los indican estos dos principales capítulos, la organización de la vigilancia y las modalidades de puesta en marcha de esta vigilancia.

Con este objetivo, indica que el control ejercido por la BEAC trata a su vez el respeto por los obligados del entorno jurídico y el entorno técnico de la emisión de moneda electrónica.

También, precisa que estos controles se ejercen con documentos e in situ. Este control de documentos in situ concierne elementos precisos:

- el número de contratos de portadores en curso;
- el número de contratos de aceptadores en curso;
- el número y el importe de las transacciones realizadas con respecto a la moneda electrónica, especialmente las cargas, las descargas y los pagos;
- el número y el importe de los incidentes de pago ocurridos;
- el saldo pendiente de la moneda electrónica emitida;
- el saldo de la cuenta «espejo» que garantiza el saldo pendiente de la moneda electrónica emitida;
- la lista de los portadores cuyos instrumentos de pago han expirado desde hace más de un mes, así como los importes que se les deben.

26. Con respecto a lo anterior, podemos destacar que esta instrucción de la BEAC no es tan completa como hubiéramos podido prever. Por otra parte, no impone obligaciones especiales en lo que se refiere a cuestiones de lucha contra el blanqueo de capitales y financiación del terrorismo.

Desde este punto de vista, tiene la misma debilidad que el resto de instrumentos BEAC en la medida que, por una parte, no conlleva disposiciones de orden general y por otra parte, no pone en marcha ningún dispositivo real limitativo sobre la cuestión del blanqueo y la financiación del terrorismo.

II- Apreciación de la legislación comunitaria CEMAC con respecto a la legislación comunitaria CEDEAO

27. De forma general, se puede considerar que el marco jurídico CEMAC es, en sus grandes directrices, cercano al marco jurídico de la CEDEAO. Esto, especialmente, con respecto a las condiciones de obtención de la autorización de ejercer o las condiciones de ejercicio en sí.

Sin embargo, analizándolo más de cerca, se pueden identificar numerosas debilidades. Estas aparecen tanto con respecto a la supervisión jurídica de la actividad de emisión de moneda electrónica como con respecto a las medidas relativas a la lucha contra el blanqueo de capitales a través de las transacciones con moneda electrónica.

28. Acerca de la supervisión jurídica de la actividad de emisión de moneda electrónica, podemos destacar:

- la vacuidad de la mayoría de las disposiciones que, de forma esencial, tienden a plantear principios genéricos sin formular reales obligaciones restrictivas;
- la tendencia al reenvío a otros textos, especialmente los de la BEAC y de la COBAC, para la elaboración de reglas precisas aplicables a las entidades de crédito en el marco de la actividad de emisión de moneda electrónica;
- la ausencia de una reglamentación precisa relativa a las relaciones con las entidades de crédito y sus socios, especialmente los portadores, salvo las reglas relativas a los contratos que los unen;
- la ausencia de obligación de control interno y la falta de precisión de la responsabilidad de las entidades emisoras con respecto a las actividades de sus socios;
- el carácter limitado de la obligación de trazabilidad, que solo es de tres (3) años, mientras que es de diez (10) años en la zona CEDEAO.
- la ausencia de una obligación de identificación de los emisores, y sobre todo, de los receptores de las transacciones con moneda electrónica;
- la ausencia de sanciones aparte de las órdenes y requerimientos o el reenvío a la aplicación de sanciones no definidas.

29. Acerca de la lucha contra el blanqueo de capitales y la financiación del terrorismo a través de transacciones con moneda electrónica.

El marco jurídico CEMAC se caracteriza por una cierta vacuidad sobre esta cuestión.

Al contrario que el marco jurídico CEDEAO, no indica claramente la obligación de los diferentes actores con las reglas comunitarias relativas al blanqueo de capitales y la financiación del terrorismo, a pesar de que sería tentador pensar que la obligación general impuesta a las entidades de crédito de sumisión a estas reglas implica su aplicación automática en este caso.

30. Además, introduce una disposición problemática y ambigua, el artículo 23 dispone entre otras cosas que: «**La COBAC fijará las reglas relativas a: (...) la lucha contra el blanqueo de capitales y la financiación del terrorismo a través de transacciones con moneda electrónica**».

En efecto, al prescribir así esta obligación de la COBAC, el reglamento da la impresión de que corresponde a la misma definir las reglas específicas mientras que habría sido más juicioso asignarle la competencia de tomar las medidas necesarias para la aplicación de la actividad de emisión de moneda electrónica del dispositivo comunitario en materia de lucha contra el blanqueo de capitales y la financiación del terrorismo.

III. Conclusión y recomendaciones

31. Finalmente, el texto de la CEMAC falla a dos niveles:

En un primer nivel, **supervisa de forma insuficiente la actividad de emisión de moneda electrónica, especialmente en lo que se refiere a la trazabilidad de las operaciones, la identificación de los emisores y receptores y la reglamentación de las relaciones entre las entidades de crédito y sus socios**, de tal forma que genera brechas para el uso malintencionado de este medio de pago.

En el segundo nivel, **establece muy vagamente la conexión entre esta actividad de emisión de moneda electrónica, el blanqueo de capitales y la financiación del terrorismo**, como si esta actividad no pudiese presentar un riesgo principal en este sentido.

32. Sin embargo, con respecto al marco jurídico CEDEAO, podemos entender este desfase.

Primero, el órgano autor del marco jurídico no es el mismo, en la medida en que el dispositivo jurídico de la CEDEAO procede directamente de un órgano técnico, la BECEAO, mientras que la CEMAC tiene un instrumento jurídico que procede de un órgano político, el Comité Ministerial.

Después, el marco jurídico CEDEAO es un marco bastante reciente, ya que data de 2015, mientras que el de la CEMAC es de 2011. Bien sabemos lo rápidas que son las evoluciones en estos ámbitos y por lo tanto, podemos entender que el marco CEMAC esté en la actualidad obsoleto.

33. Con respecto a todo lo anterior, parece urgente recomendar a las instancias de la CEMAC los elementos siguientes:

- la adopción por parte de los órganos técnicos, BEAC y COBAC, de los instrumentos jurídicos previstos en el reglamento n.º 01/11-CEMAC/UMAC/CM en sus artículos 20 a 23;
- el refuerzo en estos instrumentos jurídicos de la supervisión de la actividad de emisión de moneda electrónica según tres niveles:
 - la instauración de una trazabilidad de las operaciones durante un periodo más largo;
 - la puesta en marcha de mecanismos con el objetivo de mejorar la identificación de los emisores y de los destinatarios de las transacciones electrónicas;
 - el refuerzo del dispositivo jurídico relativo a las relaciones entre las entidades de crédito y sus socios, especialmente en lo que se refiere a sus responsabilidades en caso de uso malintencionado de estos medios de pago;
- la generalización de la obligación de declaración de las operaciones sospechosas los socios de los emisores de moneda electrónica.

Tales son, *señor Secretario Permanente*, las observaciones pertinentes que nos ha parecido necesario destacar tras este análisis de los dispositivos jurídicos CEDEAO y CEMAC con respecto a los nuevos medios de pago.

Esperando haber respondido a sus preocupaciones y cuestionamientos,

Dr. Kevin Ferdinand Njumba