Optimisation du dispositif de détection des transactions suspectes

Auteur : Efoute Nyamsi, Hélène
Promoteur(s) : Hambuckers, Julien
Faculté : HEC-Ecole de gestion de l'Université de Liège
Diplôme : Master en sciences de gestion
Année académique : 2024-2025
URI/URL : http://hdl.handle.net/2268.2/24574

MEMOIRE DE FIN D'ETUDE

En vue de l'obtention d'un diplôme de

Master en Sciences de Gestion, MBA International

Thème :

Optimisation du dispositif de détection des transactions suspectes : Étude de cas BGFIBANK Congo dans la lutte contre le blanchiment de capitaux et le financement du terrorisme (LCB-FT)

Réalisé par :

Hélène EFOUTE NYAMSI

Encadré par :

Professeur Julien HAMBRUCKERS

Année académique 2024-2025

Executive Summary

« Optimizing Suspicious Transaction Detection – BGFIBANK Congo »

Context & Objectives

- Financial institutions in Congo face growing **AML/CTF regulatory pressure** (COBAC, ANIF, GABAC, FATF standards).
- Current detection tools (AML Watch + T24) are functional but generate **high false positives** and lack advanced analytics.
- Aim: **Strengthen resilience against money laundering and terrorist financing risks** while improving operational efficiency.

Key Findings (Based on Interviews & Document Review)

1. **Technological Gaps**

- Static detection scenarios → **excessive alerts** (false positives > true cases).
- Weak integration between IT systems (AML Watch & T24).
- Lack of **AI, graph analytics, and automation**.

2. **Organizational Weaknesses**

- Silos between **compliance, operations, and commercial teams** → delays, client dissatisfaction.
- Audit function remains **reactive**, not predictive.
- Limited cross-department communication in crisis situations.

3. **Human Resource Challenges**

- **Analysts demotivated** by repetitive tasks and lack of feedback from ANIF.
- **No specialization** in transaction typologies or risk sectors.
- Low career attractiveness of compliance roles; limited access to **international certifications**.

Strategic Recommendations

A. Technological Levers

1. **AI & Machine Learning**
    - Detect anomalies beyond fixed thresholds.
    - Reduce false positives by **30–40%**.
2. **Graph Analytics**
    - Map hidden transaction networks.
    - Identify high-risk nodes (e.g., cash-intensive clients, cross-border intermediaries).
3. **Robotic Process Automation (RPA)**
    - Automate repetitive screenings, reporting, and escalation.
    - Free compliance teams for high-value investigations.

B. Organizational Levers

- Create **cross-functional AML/CTF committees** (compliance + operations + commercial).
- Implement **dynamic client risk profiling** (real-time KYC updates).
- Strengthen **three lines of defense** with clearer accountability.

C. Human Capital Levers

- Establish **specialized analyst roles** (e.g., trade finance, high-risk sectors).
- Provide **certifications** (ACAMS, ICA) and structured training programs.
- Design **career paths** to retain talent and enhance motivation.

Implementation Roadmap

1. **Short Term (0–12 months)**

- Automate routine processes (RPA).
- Launch cross-department AML committee.
- Reduce backlog of alerts.

2. **Medium Term (12–24 months)**

- Pilot AI-based detection scenarios.
- Deploy dynamic KYC tools.
- Train first cohort of certified compliance officers.

3. **Long Term (24–36 months)**

- Full integration: **AI + Graph Analytics + RPA** into a single AML platform.
- Institutionalize specialized compliance teams.
- Achieve **regional benchmark position** in AML/CTF compliance.

Expected Impact

- Reduction in false positives by up to 40%
- Faster client transaction approvals → improved satisfaction
- Enhanced collaboration between business & compliance
- Increased regulatory credibility with COBAC & ANIF
- Strengthened resilience against financial crime risks

Conclusion

Optimizing suspicious transaction detection at BGFIBANK Congo is both a regulatory imperative and a strategic opportunity.
By combining technology, organizational reform, and human capital development, the bank can transition from a reactive compliance posture to a proactive, intelligence-driven AML/CTF leader within the CEMAC region.

DÉDICACES

À mon cher Claude, Toi qui as vécu ce mémoire au quotidien, supportant mes doutes et célébrant chaque avancée. Ta force et ton amour ont été mon refuge. Sans toi, rien de tout cela n'aurait eu le même sens.

À mes enfants, Thérèse, Pauline, Kevin et Mégane, Pour tous les moments de jeu que ce travail a volé, et pour les sourires qui m'ont donné l'énergie de continuer. Puisse cet accomplissement vous inspirer à toujours aller au bout de vos rêves.

À mes très chers parents, Pour votre amour inconditionnel, vos sacrifices silencieux et les valeurs de travail et de persévérance que vous m'avez inculquées. Ce travail est le fruit de votre soutien.

À ma famille. Pour avoir cru en moi et pour m'avoir encouragé avec patience et affection tout au long de cette aventure.

REMERCIEMENTS

Au terme de ce long travail de recherche, il m'est agréable de respecter la tradition en adressant mes plus sincères remerciements à tous ceux qui ont contribué, de près ou de loin, à l'aboutissement de ce mémoire.

En tout premier lieu, je souhaite exprimer ma plus profonde gratitude à mon directeur de mémoire, **le Professeur Julien HAMBRUCKERS**. Sa rigueur scientifique, sa grande disponibilité et ses conseils avisés ont été des guides précieux tout au long de cette année. Je le/la remercie pour sa patience, ses relectures attentives et pour la confiance qu'il/elle a placée dans mon travail.

Mes remerciements s'adressent également aux membres du jury pour l'honneur qu'ils me font en acceptant d'évaluer ce travail et pour le temps précieux qu'ils y consacrent.

Je tiens à remercier très chaleureusement l'ensemble de l'institution **BGFIBANK CONGO** pour m'avoir accueilli en son sein. J'exprime ma reconnaissance à la **Direction Générale** pour avoir rendu cette étude possible. Mes remerciements vont tout particulièrement au **Directeur de la Conformité** pour son soutien constant et pour avoir facilité l'aboutissement de ce travail. J'associe à ces remerciements l'ensemble **des collaborateurs du département Conformité** pour leur accueil, leur esprit d'équipe et leur précieuse collaboration.

Je remercie également l'ensemble du corps professoral et administratif de **HEC LIEGE** dont les enseignements et le soutien ont été fondamentaux dans mon parcours.

Enfin, sur un plan plus personnel, je souhaite remercier du fond du cœur ma famille. Mes parents, pour leur amour et leur soutien indéfectible depuis toujours. **Mon conjoint Claude**, pour sa patience infinie et ses encouragements dans les moments de doute. Mes frères et sœurs, ainsi que mes amis, qui ont su m'apporter le soutien moral nécessaire pour mener à bien ce projet de longue haleine.

À tous, merci.

RÉSUMÉ

Ce mémoire s'inscrit dans le cadre de l'étude approfondie des dispositifs de lutte contre le blanchiment de capitaux et le financement du terrorisme (LCB-FT), en se concentrant sur l'efficacité de la détection des transactions suspectes. Il prend pour étude de cas la BGFIBANK Congo, acteur majeur du secteur bancaire en Afrique centrale. La problématique de cette recherche repose sur l'adéquation entre les exigences réglementaires, les menaces émergentes et la capacité technologique des institutions bancaires à détecter de manière proactive les activités suspectes.

La recherche combine une revue documentaire, des entretiens semi-directifs et une analyse critique des pratiques existantes. À travers un diagnostic approfondi, elle identifie les forces et faiblesses du dispositif actuel de la BGFIBANK Congo. Ensuite, des leviers technologiques (intelligence artificielle, analyse de graphes, machine learning), organisationnels (culture de conformité, gouvernance) et humains (formation, spécialisation) sont proposés afin d'optimiser le système existant.

Ce travail propose également un plan d'action concret, phasé sur trois ans, accompagné d'indicateurs de performance et d'un système de suivi. Il contribue ainsi à renforcer la résilience bancaire face aux risques de blanchiment et de financement du terrorisme, tout en alignant les pratiques locales sur les standards internationaux.

Mots-clés : LCB-FT, transactions suspectes, BGFIBANK Congo, intelligence artificielle, analyse de graphes, conformité bancaire, CEMAC, COBAC, ANIF.

ABSTRACT

This thesis focuses on enhancing the detection mechanisms for suspicious transactions, within the broader framework of Anti-Money Laundering and Counter-Terrorist Financing (AML-CTF) systems. It takes BGFIBANK Congo as a case study, a key financial player in Central Africa. The core research question centers on the alignment between regulatory requirements, emerging threats, and the technological capacity of banks to proactively identify suspicious financial behavior.

The methodology integrates documentary analysis, semi-structured interviews, and critical benchmarking of current practices. Through a comprehensive diagnosis, the study identifies the strengths and weaknesses of BGFIBANK Congo's current AML-CTF system. It then proposes technological (AI, graph analytics), organizational (compliance governance, interdepartmental collaboration), and human (training, specialization) levers to optimize the detection processes.

The study concludes with a concrete implementation roadmap over a three-year period, with measurable KPIs and monitoring mechanisms. It aims to strengthen financial institutions' resilience to illicit financial risks, while aligning local practices with international standards.

Keywords : AML-CTF, suspicious transactions, BGFIBANK Congo, artificial intelligence, graph analytics, banking compliance, CEMAC, COBAC, ANIF.

INTRODUCTION GÉNÉRALE

Contexte et enjeux mondiaux de la LCB-FT

Dans un contexte mondial marqué par l'intensification des flux financiers transnationaux, la mondialisation des échanges et la digitalisation croissante des services bancaires, les menaces liées au blanchiment de capitaux et au financement du terrorisme (LCB-FT) constituent des enjeux majeurs pour la stabilité financière, la sécurité des États et la crédibilité des institutions bancaires. Selon le Fond Monétaire International (FMI), le blanchiment de capitaux représenterait entre 2 % et 5 % du PIB mondial chaque année, soit entre 800 et 2 000 milliards de dollars (*FMI, 2022*). Le financement du terrorisme, bien que souvent moins volumineux, est tout aussi destructeur, car il alimente des réseaux criminels, extrémistes et géopolitiquement sensibles.

Face à cette menace systémique, la communauté internationale s'est dotée de plusieurs cadres normatifs, notamment les 40 recommandations du Groupe d'Action Financière (GAFI), qui imposent aux États membres de mettre en place des dispositifs robustes de détection, d'analyse et de signalement des transactions suspectes. À ces exigences s'ajoutent les résolutions du Conseil de sécurité de l'ONU, les normes du Comité de Bâle, et celles des organismes régionaux comme le GIABA en Afrique de l'Ouest ou le GABAC en Afrique centrale.

Problématique de la détection des transactions suspectes en Afrique centrale

Malgré la transposition progressive de ces standards internationaux, l'Afrique centrale demeure vulnérable face aux risques de blanchiment et de financement illicite. La région souffre de plusieurs handicaps structurels : faiblesse institutionnelle, insuffisance des ressources humaines spécialisées, prédominance du cash, faible bancarisation, porosité des frontières, et pression politique sur les autorités de supervision.

Dans ce contexte, la détection des transactions suspectes – pierre angulaire de tout dispositif LCB-FT – pose un véritable défi. Les banques, souvent démunies face à la sophistication croissante des montages financiers illicites, peinent à concilier respect réglementaire, efficacité opérationnelle et gestion des faux positifs. À titre d'exemple, plus de 80 % des alertes générées par les systèmes automatiques dans les banques africaines ne débouchent sur aucune déclaration pertinente, selon une étude conjointe de la Banque mondiale et du GAFI (2023).

C'est dans ce cadre que s'inscrit l'étude du cas BGFIBANK Congo, une banque de référence dans la sous-région CEMAC, qui se trouve au carrefour de plusieurs enjeux : exigences de conformité croissantes, transformation digitale, attentes sociétales en matière de gouvernance, et exposition au risque réputationnel.

Justification scientifique et pratique de l'étude

D'un point de vue scientifique, cette recherche s'inscrit dans une dynamique interdisciplinaire, à la croisée de la finance, de la technologie, du droit bancaire et de la gestion des risques. Elle vise à enrichir les réflexions sur les approches innovantes de détection des flux illicites, en intégrant les apports récents de l'intelligence artificielle, de l'analyse comportementale et de l'automatisation des processus.

Sur le plan pratique, l'étude propose un cadre d'analyse opérationnel et contextualisé, capable de servir d'outil d'aide à la décision pour les responsables de la conformité bancaire. En identifiant les dysfonctionnements actuels et en formulant des recommandations concrètes, elle vise à renforcer l'efficience du système de détection, tout en limitant les coûts de mise en conformité.

BGFIBANK Congo, par son positionnement stratégique et sa volonté affichée de modernisation, constitue un terrain d'étude idéal pour tester l'applicabilité et la performance des leviers technologiques, organisationnels et humains au service de la LCB-FT.

Objectifs généraux et spécifiques

Objectif général :

Optimiser le dispositif de détection des transactions suspectes au sein de BGFIBANK Congo, dans une perspective de conformité renforcée aux standards internationaux LCB-FT.

Objectifs spécifiques :

- Analyser le cadre réglementaire et technologique applicable à la détection des transactions suspectes en Afrique centrale ;
- Diagnostiquer le dispositif existant de BGFIBANK Congo à travers une grille d'évaluation multicritères ;
- Identifier les lacunes, inefficacités ou risques systémiques liés à l'approche actuelle ;
- Proposer des leviers d'optimisation intégrant des outils d'intelligence artificielle, des pratiques organisationnelles modernes et des mécanismes de formation continue ;
- Élaborer un plan de mise en œuvre structuré, assorti d'indicateurs de performance.

Hypothèses de recherche

- H1 : Le dispositif actuel de détection des transactions suspectes de BGFIBANK Congo présente des limites techniques et organisationnelles freinant son efficacité.
- H2 : L'intégration d'outils d'intelligence artificielle et d'analyse de graphes peut significativement améliorer la détection proactive et réduire les faux positifs.
- H3 : Un renforcement des capacités humaines (formation, spécialisation) et des processus internes peut accroître la réactivité et la précision des alertes.
- H4 : La gouvernance de la conformité bancaire, lorsqu'elle est intégrée transversalement, favorise une meilleure résilience face aux risques LCB-FT.

Méthodologie de recherche et limites

Cette recherche adopte une approche mixte, combinant méthodologie qualitative (entretiens, observation participante) et analyse documentaire approfondie.

- Sources de données :

Rapports réglementaires (GAFI, COBAC, ANIF)

Documentation interne de BGFIBANK Congo

Études académiques et sectorielles

Retours d'expérience de professionnels de la conformité

- Méthodes d'analyse :

Analyse SWOT du dispositif existant

Benchmark international des meilleures pratiques

Étude de cas approfondie

Recommandations structurées selon une grille technologique / organisationnelle / humaine

- Limites de l'étude :

Accès restreint à certaines données confidentielles internes à la banque

Taille limitée de l'échantillon d'entretiens

Possible biais de perception des acteurs interrogés

Données statistiques parfois manquantes ou non harmonisées au niveau régional

Structure de la thèse

Le travail est structuré en trois parties principales :

Partie I : exposition du cadre théorique, réglementaire et technologique entourant la LCB-FT ;

Partie II : diagnostic détaillé du dispositif de détection en place à BGFIBANK Congo ;

Partie III : recommandations stratégiques et plan d'action priorisé.

Chaque partie est subdivisée en chapitres, avec des figures, tableaux et études de cas, pour permettre une compréhension progressive et approfondie des problématiques.

PARTIE I – Cadre conceptuel, réglementaire et technologique

La mise en place d'un dispositif efficace de détection des transactions suspectes repose sur une compréhension rigoureuse de ses fondements conceptuels, juridiques et technologiques. Avant d'analyser le cas spécifique de BGFIBANK Congo, il est indispensable de situer le cadre dans lequel évoluent les systèmes LCB-FT, tant du point de vue de la **typologie des risques**, que des **normes réglementaires internationales et régionales**, ainsi que des **outils techniques mobilisables**.

Cette première partie de la thèse vise à fournir un socle de connaissances solides et interconnectées, structuré autour de quatre dimensions essentielles :

- Le **chapitre 1** introduit les notions fondamentales relatives au blanchiment de capitaux, au financement du terrorisme, à la notion de transaction suspecte et à leurs implications pour les institutions financières. Il présente également les typologies de risque et les impacts juridiques, opérationnels et réputationnels associés.
- Le **chapitre 2** dresse un panorama du cadre réglementaire applicable, en partant des recommandations du GAFI jusqu'aux obligations imposées par la COBAC et l'ANIF, tout en mettant en perspective le positionnement de la République du Congo face aux standards internationaux.
- Le **chapitre 3** explore les dispositifs de détection, en comparant les méthodes traditionnelles aux innovations récentes telles que l'intelligence artificielle, l'analyse de graphes ou encore l'automatisation des flux par RPA.
- Enfin, le **chapitre 4** présente les bonnes pratiques et modèles organisationnels observés dans des banques internationales, avec l'objectif de nourrir une réflexion sur la transposition de ces éléments dans un contexte bancaire africain.

Ce cadre analytique pluridimensionnel permet non seulement de situer les enjeux techniques et stratégiques de la conformité LCB-FT, mais sert également de base à l'évaluation critique du dispositif en vigueur au sein de BGFIBANK Congo, qui sera conduite dans la seconde partie de ce travail.

Chapitre 1 – Concepts fondamentaux et risques associés

La compréhension des risques liés au blanchiment de capitaux et au financement du terrorisme (BC/FT) constitue un préalable indispensable à la mise en place d'un dispositif efficace de détection et de prévention dans le secteur bancaire. Ce chapitre vise à poser les bases conceptuelles de la recherche, en définissant les termes clés, en expliquant les processus typiques du blanchiment, en identifiant les spécificités du financement du terrorisme, en posant les base d'identification d'une transaction suspecte et en analysant les conséquences que ces activités illicites font peser sur les institutions financières.

4. Définition du blanchiment de capitaux et du financement du terrorisme

a. Définitions juridiques et normes internationales

Le blanchiment d'argent fait référence au processus par lequel des individus ou des entités dissimulent l'origine des produits obtenus illicitement afin qu'ils semblent légitimes après être passés par une série de transactions financières. L'objectif fondamental est d'intégrer ces fonds dans l'économie formelle sans éveiller la suspicion. Le financement du terrorisme, bien qu'il soit souvent lié à des méthodes similaires, diffère dans ses intentions, car il implique la fourniture de fonds pour des actes ou des organisations terroristes, que la source de ces fonds soit légale ou illégale (Utkina et al., 2023). Les deux concepts ont des interprétations juridiques distinctes d'une administration à l'autre, mais sont unifiés par des cadres internationaux qui tentent de normaliser les définitions et les approches d'application de la loi. Au niveau international, des organismes tels que le Groupe d'action financière (GAFI) ont émis des recommandations visant à harmoniser les mesures nationales de LBC/FT. Ces recommandations énoncent des définitions explicites et définissent les responsabilités institutionnelles en matière de détection, de prévention et de poursuite des infractions liées au blanchiment d'argent et au financement du terrorisme. Un élément essentiel des orientations du GAFI est le maintien d'une séparation claire des rôles, en particulier pour s'assurer que les auditeurs internes restent indépendants des fonctions opérationnelles lorsqu'ils évaluent les contrôles LBC/FT. Cette exigence répond aux préoccupations concernant l'objectivité compromise qui peuvent survenir si les auditeurs participent à la conception ou à l'exécution des procédures qu'ils inspectent par la suite. De nombreux pays intègrent les normes du GAFI dans leurs régimes législatifs et réglementaires, en les adaptant aux contextes locaux. Par exemple, le cadre législatif du Nigéria comprend la loi sur la lutte contre le blanchiment d'argent et le financement du terrorisme, ainsi que d'autres institutions de soutien telles que la Cellule de renseignement financier du Nigéria. Cependant, bien qu'il ait adopté de telles mesures dès 2004, le Nigeria reste répertorié par le GAFI comme présentant des défaillances stratégiques dans son régime de LBC/FT (Akinteye et al., 2023). Cela reflète des lacunes persistantes dans la mise en œuvre, soulignant que l'adoption légale ne garantit pas à elle seule une application efficace. Dans l'ensemble des juridictions, la surveillance financière fait partie intégrante des objectifs plus larges de la lutte contre le blanchiment d'argent. Les définitions juridiques consacrent souvent des obligations de surveillance exigeant des institutions qu'elles observent en permanence le comportement transactionnel des clients et signalent les tendances suspectes aux autorités compétentes (Utkina et al., 2023). En termes pratiques, cette obligation se manifeste par des rapports d'activités suspectes (SAR) dans de nombreux systèmes, avec des délais réglementaires clairs pour le dépôt et des seuils définis pour ce qui déclenche le signalement. Le financement du terrorisme fait également l'objet d'une attention particulière en vertu des normes internationales en raison de ses conséquences potentielles sur la sécurité nationale et mondiale.

Contrairement au blanchiment d'argent, où l'origine des fonds est toujours illicite, les lois sur le financement du terrorisme étendent leur champ d'application pour couvrir les avoirs provenant de sources légitimes s'ils sont utilisés pour planifier ou exécuter des actes terroristes. Le GAFI reconnaît explicitement cette portée plus large dans ses recommandations, en mettant l'accent sur les mesures préventives dans les systèmes bancaires et les services financiers non bancaires. Les développements récents soulignent à quel point des événements géopolitiques tels que la pandémie de COVID-19 créent de nouvelles vulnérabilités dans les deux domaines. Des normes juridiquement contraignantes mettent désormais l'accent sur l'adaptation des évaluations des risques à l'échelle nationale et internationale au lieu d'appliquer des solutions uniformes sans tenir compte des menaces propres à chaque juridiction (Ryder, s.d.). Ce changement signale une évolution dans la façon dont les cadres juridiques opérationnalisent les approches fondées sur les risques défendues par les directives du GAFI. Un autre aspect central des définitions mondiales de LBC/FT concerne la collaboration multisectorielle que le GAFI promeut dans le cadre de son modèle de partenariat. Le principe suppose ici que les acteurs privés, tels que les banques, possèdent déjà des informations vitales sur les clients susceptibles d'aider les forces de l'ordre si elles sont partagées de manière responsable (Helgesson & Mörth, 2018). Les normes juridiques officialisent de plus en plus ce partage par le biais de protocoles d'entente entre les organismes de réglementation, les cellules de renseignement financier et les équipes de conformité privées, tout en équilibrant les préoccupations relatives à la protection de la vie privée. Compte tenu de ces normes internationales, les normes établissent également des distinctions entre les fonctions d'enquête telles que la juricomptabilité et l'audit général. Bien qu'ils soient interconnectés dans leurs capacités de détection des fraudes, ces rôles ne sont pas interchangeables selon la plupart des définitions réglementaires en raison des différences de portée et d'admissibilité des éléments de preuve générés au cours des enquêtes (Efuntade et Efuntade, 2023). Le législateur codifie ces limites afin d'en assurer l'application appropriée, selon qu'une affaire nécessite un examen préventif ou un examen a posteriori en vue d'éventuelles poursuites. L'amélioration continue des définitions juridiques s'accompagne d'évolutions technologiques qui influencent la manière dont la conformité aux normes est assurée. L'analytique basée sur l'IA complétant la surveillance humaine dans les systèmes de surveillance des transactions, les législateurs commencent à envisager des exigences légales spécifiques en matière de transparence des algorithmes et d'atténuation des biais (Palakurti, 2023). Bien que les recommandations actuelles du GAFI ne prescrivent pas de technologies particulières, elles exigent le respect de principes tels que la précision, la rapidité des efforts de détection et l'adaptabilité aux typologies émergentes, le tout potentiellement aidé par des méthodes de calcul avancées lorsqu'elles sont correctement gérées. L'interaction entre les recommandations mondiales et le droit national crée une matrice où les obligations en matière de LBC/FT s'appliquent à plusieurs niveaux. À la base, il reste des points d'ancrage clairs : le blanchiment d'argent se concentre sur l'obscurcissement des origines illicites ; Le financement du terrorisme se concentre sur le financement d'actes illégaux, quelle que soit leur légalité. Ces points d'ancrage s'articulent autour de cadres qui obligent à identifier de manière proactive les menaces au moyen de mécanismes de signalement normalisés, de fonctions d'examen indépendantes au sein des institutions, d'une coordination structurée entre les secteurs et d'une utilisation ciblée d'aides technologiques, le tout visant à combler les lacunes procédurales par lesquelles les flux financiers illicites pourraient autrement passer inaperçus.

b. Caractéristiques et typologies clés

L'identification des caractéristiques déterminantes et des typologies récurrentes du blanchiment de capitaux et du financement du terrorisme est cruciale pour développer des contre-mesures ciblées. Les deux activités utilisent des voies de transaction en couches pour dissimuler leur objectif réel, mais les distinctions fondamentales résident dans l'origine, l'intention et l'adaptation opérationnelle aux pressions

contextuelles. Le blanchiment d'argent implique universellement des fonds d'origine illicite, qui passent par une séquence d'étapes de placement, de superposition et d'intégration pour masquer leur provenance. L'étape de placement peut impliquer des dépôts physiques ou des virements numériques sur des comptes bancaires, souvent structurés pour éviter les déclencheurs de détection tels que les seuils de déclaration. La superposition introduit plusieurs mouvements rapides entre les comptes, les juridictions ou les classes d'actifs pour perturber les pistes d'audit. L'intégration réintroduit ensuite ces fonds dans l'économie légitime par le biais d'investissements ou d'achats de grande valeur qui semblent légaux (Utkina et al., 2023). Le financement du terrorisme n'a pas besoin d'être d'origine illicite ; Les flux de revenus légaux peuvent être détournés pour soutenir les aspects opérationnels ou logistiques du terrorisme. Cette distinction signifie que les approches traditionnelles de lutte contre le blanchiment d'argent axées uniquement sur l'identification des produits de la criminalité peuvent ne pas détecter les flux de financement liés au terrorisme lorsqu'ils proviennent de sources apparemment propres. Le caractère opportuniste des méthodes de financement du terrorisme renforce cette complexité. Plutôt que d'être à l'avant-garde de mécanismes de transfert fondamentalement nouveaux, les acteurs cooptent souvent les structures économiques existantes, telles que les organismes de bienfaisance, les organismes à but non lucratif, les réseaux commerciaux ou les services de transfert de fonds, en exploitant les angles morts réglementaires ou les changements induits par la crise dans les modèles financiers (Ryder, n.d.). Par conséquent, l'identification de ces activités nécessite une analyse axée sur les indicateurs de destination et d'intention plutôt que sur la simple légalité des sources de financement. Les manifestations typiques du blanchiment d'argent au sein des systèmes bancaires comprennent des pics soudains de volumes de transactions incompatibles avec l'activité historique des comptes, des transferts transfrontaliers fréquents impliquant des juridictions connues pour leurs lois sur le secret ou l'utilisation de plusieurs comptes intermédiaires sans justification commerciale claire. La détection de ces comportements bénéficie de l'intégration d'informations comportementales dans les modèles de surveillance. En capturant les écarts par rapport aux habitudes de dépenses de base et en intégrant des variables telles que la géographie des transactions, les catégories de commerçants et le regroupement temporel des paiements dans les systèmes pilotés par l'IA, les institutions peuvent améliorer la détection des anomalies au-delà des alertes fixes basées sur des règles. Pour les typologies de financement du terrorisme, on préfère souvent les transactions petites à modérées dispersées dans le temps afin de minimiser le risque de détection. Dans de nombreux cas, les fonds sont acheminés par le biais de comptes personnels, de façades commerciales proposant des opérations à forte intensité de liquidités (par exemple, les agences de voyages) ou de la liquidation d'actifs au sein d'économies informelles. L'utilisation de canaux licites complique la distinction entre les activités légitimes et suspectes. Là encore, la compréhension des tendances comportementales, telles que les changements soudains dans les profils des bénéficiaires des transactions alignés sur les lieux extrémistes connus, ajoute une couche prédictive à l'évaluation des risques (Palakurti, 2023). Du point de vue de la conformité institutionnelle, la reconnaissance de la typologie est tout aussi pertinente pour façonner le contenu des rapports d'activités suspectes. Les systèmes de surveillance des transactions ancrés dans l'analyse du Big Data s'attaquent à ce problème en traitant en permanence des informations en temps réel provenant de sources variées afin de mettre en évidence des cas potentiels basés à la fois sur des anomalies structurées et des associations de modèles non structurés (Ji, 2023). Les techniques d'apprentissage automatique non supervisées peuvent révéler des groupes de transactions liées sans être étiquetées au préalable comme suspectes ou authentiques ; ces résultats peuvent révéler des relations cachées, telles que des adresses IP partagées dans des transactions en ligne ou des détails de bénéficiaire qui se chevauchent dans des comptes apparemment sans rapport. Les outils de visualisation avancés améliorent encore la découverte de motifs, ce qui est essentiel à l'identification de la typologie. La cartographie des nœuds transactionnels à travers des graphes de réseau permet de visualiser les comptes intermédiaires centraux agissant comme des plaques tournantes pour les systèmes de blanchiment distribué. De même, les cartes thermiques représentant des irrégularités géographiquement concentrées peuvent signaler l'existence de réseaux de blanchiment coordonnés exploitant les vulnérabilités régionales. Pour les scénarios de financement du terrorisme impliquant des transferts dispersés de faible valeur associés à des points chauds de radicalisation, les visualisations de séries chronologiques aident les analystes à relier les pics épisodiques entre différents profils de clients. Les criminels qui s'adaptent opérationnellement exploitent des faiblesses propres à des secteurs autres que le secteur bancaire formel où les mécanismes de surveillance diffèrent. Le blanchiment d'argent basé sur le commerce illustre l'un de ces modèles : une fausse déclaration

intentionnelle sur le prix, la quantité ou la qualité des importations et des exportations facilite le transfert de valeur sous le couvert de transactions commerciales. Bien qu'elles soient souvent liées à des syndicats du crime organisé à la recherche d'opportunités de recyclage des profits, des tactiques similaires ont été identifiées dans la collecte de fonds pour le terrorisme où la sous-facturation ou la surfacturation fournit des canaux de financement secrets. Les praticiens de la lutte contre le blanchiment d'argent et le financement du terrorisme notent également des typologies hybrides où le blanchiment des produits du crime et les transferts axés sur le terrorisme se mélangent au sein de flux complexes conçus pour servir simultanément plusieurs objectifs. Par exemple, les revenus du trafic de stupéfiants peuvent être partiellement remis à des alliés idéologiques engagés dans la violence politique, tandis que d'autres parties sont réintégrées localement en tant que profit commercial légitime, un scénario à double usage compliquant les modèles de détection orientés vers des motivations singulières. Les réponses institutionnelles doivent refléter ces nuances grâce à des architectures de conformité adaptables qui allient surveillance automatisée et jugement humain éclairé (Palakurti, 2023). Une dépendance excessive à l'automatisation risque d'être mal classée si les machines sont formées exclusivement sur des profils historiques qui ne tiennent pas compte de l'innovation émergente dans les tactiques de superposition (Paul et al., 2023). À l'inverse, l'examen manuel non assisté limite l'évolutivité par rapport aux volumes de transactions modernes. La combinaison de la reconnaissance de formes computationnelle et de l'analyse contextuelle de l'enquêteur permet à la fois la précision du signalement des soupçons et la faisabilité opérationnelle. Dans le paysage du blanchiment d'argent et du financement des activités terroristes, il existe un état perpétuel de flux tactique où les délinquants modifient leurs méthodes en réponse à des pressions externes telles qu'une réglementation plus stricte ou des mises à niveau technologiques de l'application de la loi. Ce dynamisme souligne pourquoi les listes de contrôle statiques des signaux d'alarme des transactions sont insuffisantes ; Les cadres de typologie doivent évoluer en permanence en intégrant de nouvelles études de cas partagées entre les autorités publiques telles que les cellules de renseignement financier et les équipes de conformité du secteur privé (Godefroy et al., 2011). Le partage collaboratif de l'intelligence permet de combler les asymétries dans la connaissance de la typologie tout en offrant des alertes précoces concernant les nouveaux programmes en incubation à l'étranger mais potentiellement transférables localement. En fin de compte, les caractéristiques qui sous-tendent la plupart des typologies reposent sur des efforts de dissimulation visant soit l'origine des fonds (dans le domaine du blanchiment), soit à des fins de fonds (dans le financement du terrorisme). Pour les détecter, il faut opérationnaliser des attributs nuancés, des marqueurs d'incohérence comportementale, des liens de réseau entre des entités apparemment indépendantes, un obscurcissement délibéré par des intermédiaires, et les comparer à des classifications d'apprentissage automatique adaptatives capables de capturer des séquences de paiement non conventionnelles sans codage de règles explicites préalables (Palakurti, 2023).

c. Différences et chevauchements entre le blanchiment de capitaux et le financement de terrorisme

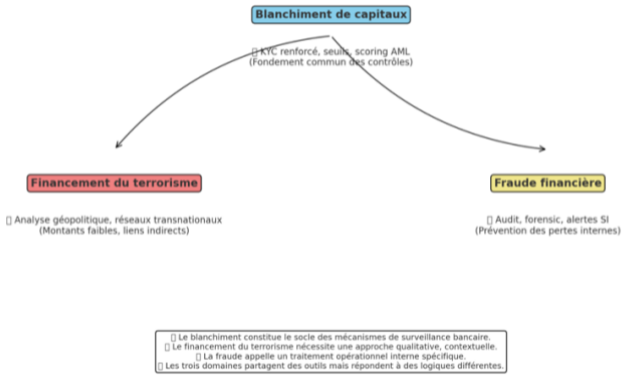
Bien que le blanchiment d'argent et le financement des activités terroristes soient tous deux des crimes financiers impliquant des tentatives délibérées de dissimuler des pistes transactionnelles, leurs objectifs sous-jacents diffèrent fondamentalement, mais présentent des similitudes opérationnelles notables. Dans le ML, l'objectif principal est de transformer des fonds obtenus illicitement en actifs qui semblent avoir des origines légitimes. Ce processus passe généralement par des étapes identifiables : le placement dans le système financier, la superposition pour dissimuler la piste d'audit à travers une série de transactions complexes, et l'intégration où les fonds retournent dans une circulation économique légale sous un déguisement apparemment légitime (Utkina et al., 2023). En revanche, le Fonds pour l'exportation se concentre sur l'utilisation de ressources, licites ou illicites, pour financer des activités qui soutiennent le terrorisme. Par conséquent, alors que le ML commence toujours par les produits criminels, le FT peut provenir de gains légaux détournés ultérieurement à des fins illégales. La divergence des origines influence naturellement les approches de détection. Les cadres de lutte contre le blanchiment d'argent se concentrent souvent sur le traçage des flux entrants suspects qui signalent une possible provenance criminelle. Dans les cas de FTF, cependant, la détection basée sur l'origine peut échouer, car les fonds peuvent initialement provenir de salaires, de dons de bienfaisance ou de revenus commerciaux légaux

(Ryder, s.d.). Les mesures réglementaires mettent donc l'accent non seulement sur l'origine des fonds, mais aussi sur l'utilisation finale prévue lorsqu'elles luttent contre le financement du terrorisme. De ce point de vue, l'une des principales différences réside dans la portée de la définition juridique : les lois sur le blanchiment d'argent ciblent étroitement l'origine illicite de flux de capitaux, tandis que les lois sur le financement du terrorisme englobent tout financement lorsqu'il est démontrable que le destinataire ou l'objectif correspond aux objectifs de l'activité terroriste. Malgré ces différences dans l'intention et la typologie des sources, il existe un chevauchement important entre les méthodologies utilisées par les auteurs. Les deux crimes exploitent les faiblesses des systèmes de surveillance financière en fragmentant les flux de transactions entre les institutions et les juridictions avec des niveaux variables de rigueur réglementaire. Des mécanismes tels que le blanchiment basé sur le commerce, où les marchandises sont surfacturées ou sous-facturées pour déplacer secrètement de la valeur, ou l'utilisation d'entreprises à forte intensité de liquidités comme façades s'appliquent à la fois au blanchiment de capitaux et au financement du terrorisme (Utkina et al., 2023). Les criminels adaptent ces mécanismes en fonction des contraintes conjoncturelles ; Par exemple, un réseau principalement engagé dans le blanchiment de produits peut allouer une fraction de ses fonds à des alliés idéologiques engagés dans des opérations terroristes, créant ainsi des flux financiers hybrides qui fusionnent des éléments des deux infractions. Structurellement, ces chevauchements présentent des défis pour les systèmes de surveillance, car les modèles de transaction peuvent sembler indiscernables sans intelligence contextuelle concernant les affiliations des acteurs ou la géographie opérationnelle connue. Par exemple, les micro-transferts rapides en dessous des seuils de déclaration pourraient signifier une structuration dans des systèmes de blanchiment destinés à éviter la détection ou être une technique employée par les financiers du terrorisme cherchant à accumuler des fonds supplémentaires sans déclencher d'alertes (Palakurti, 2023). Les deux contextes nécessitent une capacité d'analyse pour détecter des anomalies comportementales cohérentes telles que des transferts répétitifs entre les mêmes contreparties en l'absence de justifications commerciales claires. Le recours commun à des techniques de camouflage complique encore la différenciation des enquêtes. Le recours à des intermédiaires, qu'il s'agisse de personnes agissant en tant que mules ou de sociétés écrans constituées dans des juridictions clémentes, reste essentiel pour dissiper les liens directs entre le donneur d'ordre et le bénéficiaire final (Kannan et al., 2022). Pour les opérations de ML, cela rompt les liens entre les fonds et les crimes sous-jacents tels que le trafic de drogue ou la corruption ; pour TF, il obscurcit les liens possibles avec des organisations ou des personnes désignées. De plus, la structuration stratifiée des transactions à travers plusieurs classes d'actifs, les conversions de devises, les mouvements entre les comptes bancaires et les cryptomonnaies, l'acquisition de biens portables de grande valeur, servent les deux objectifs en ajoutant de la complexité qui met à rude épreuve la traçabilité. Les institutions financières sont donc confrontées à des décisions stratégiques importantes sur la manière de concevoir l'architecture de surveillance. Les systèmes basés sur des règles et calibrés exclusivement sur des anomalies typiques du ML risquent de manquer des modèles TF dont les signatures peuvent impliquer des transferts à petite échelle mais très contextuels (Palakurti, 2023). À l'inverse, les configurations qui optimisent les signaux d'alarme TF peuvent surcharger les analystes de faux positifs si elles ne sont pas correctement réglées contre les signatures de blanchiment de valeur plus importante. Les institutions alignent ces contrôles sur des obligations plus larges en matière de LBC/FT définies par des normes internationales telles que les recommandations du GAFI et appliquées au niveau national par le biais d'une législation adaptée (Quintel, 2022). Les implications du risque opérationnel découlant à la fois du ML et du FT convergent pour les banques. Des défaillances dans les processus conçus pour détecter les activités inhabituelles peuvent permettre à l'un ou l'autre type de flux de ne pas être détecté, comme en témoignent les défaillances très médiatisées où une intégration procédurale défectueuse a permis le passage transfrontalier de fonds suspects. Les défaillances se produisent non seulement au niveau des processus, mais aussi aux niveaux de gouvernance lorsque les conseils de surveillance ne garantissent pas de ressources suffisantes pour les fonctions de conformité ou ne tolèrent pas les défaillances systémiques contraires aux mandats politiques (McConnell, 2020). Les initiatives intersectorielles répondent à cette convergence en favorisant le partage de renseignements au-delà des frontières public-privé, de sorte que les typologies rencontrées dans un domaine informent les paramètres de détection de l'autre (LAPTEş, 2023). Les modifications réglementaires officialisent de plus en plus les canaux de coopération, permettant aux forces de l'ordre d'accéder aux données transactionnelles pertinentes pour les deux crimes, tout en protégeant le droit à la vie privée. Cette pratique reconnaît que la reconnaissance rapide des points de chevauchement favorise l'allocation des

ressources : les renseignements sur les cas recueillis au cours d'une enquête sur le blanchiment d'argent peuvent révéler des liens associatifs pointant vers des activités liées au terrorisme nécessitant une action d'interdiction immédiate. Les interventions technologiques renforcent cette interaction entre les régimes préventifs. Les modèles d'apprentissage automatique capables d'intégrer l'analyse comportementale évaluent de manière comparative à la fois les anomalies de transaction de grande valeur caractéristiques du blanchiment et les modèles dispersés de faible valeur indiquant une activité liée au terrorisme (Palakurti, 2023). La combinaison de ces analyses et de la surveillance interprétative humaine peut combler des lacunes là où la détection automatisée seule aurait du mal en raison d'une connaissance contextuelle insuffisante. De plus, les outils de visualisation des données aident les analystes à cartographier les réseaux relationnels où les entités examinées sont liées à la fois par des stratagèmes d'enrichissement illicite et des canaux de soutien extrémistes, une intersection graphique cruciale pour l'atténuation des menaces polyvalentes. En fin de compte, l'appréciation des distinctions et des intersections entre le blanchiment d'argent et le financement du terrorisme revêt une importance opérationnelle non seulement pour la clarté des définitions, mais aussi pour les stratégies pratiques de dissuasion. Les institutions financières comme BGFIBANK Congo doivent calibrer les systèmes de surveillance suffisamment souples pour naviguer dans ces caractéristiques qui se chevauchent tout en conservant une spécificité sur les marqueurs de risque distincts pertinents pour chaque domaine (Utkina et al., 2023). Ce faisant, l'intégrité de la conformité tout en améliorant la résilience face à l'exploitation par diverses formes de criminalité financière qui peuvent adopter des façades similaires malgré des objectifs finaux différents.

Tableau 1: Différences clés entre blanchiment et financement du terrorisme

Critère	Blanchiment de capitaux	Financement du terrorisme
Objectif	Dissimuler l'origine des fonds	Soutenir une activité terroriste
Origine des fonds	**Toujours illégale**	**Légale ou illégale**
Détection	Basée sur la traçabilité des fonds	Basée sur l'analyse des finalités et des bénéficiaires
Risque pour les banques	Risque juridique et réputationnel	Risque de sanctions internationales graves



Interconnexion des traitements bancaires : Blanchiment, Terrorisme et Fraude

5. Théories de la criminalité économique et financière

a. Théorie du choix rationnel dans les crimes financiers

La théorie du choix rationnel offre une lentille structurée à travers laquelle les motivations et les processus de prise de décision des individus qui se livrent à des crimes financiers, y compris le blanchiment d'argent (BC) et le financement du terrorisme (FT), peuvent être interprétés. À la base, la théorie postule que les acteurs se comportent comme des agents rationnels qui évaluent systématiquement les actions potentielles en pesant les avantages attendus par rapport aux coûts anticipés. La décision de commettre un crime financier survient lorsque les récompenses perçues l'emportent sur les risques associés tels que la détection, les sanctions juridiques ou l'atteinte à la réputation. Ce cadre suppose que les délinquants ont une connaissance, éclairée ou intuitive, des mécanismes d'application de la loi et qu'ils adaptent leur comportement en conséquence afin de maximiser leur gain personnel ou leur impact idéologique. Dans cette perspective, les acteurs du blanchiment de capitaux peuvent choisir des techniques de blanchiment en fonction de leur efficacité à dissimuler les produits illicites tout en minimisant l'exposition. Les variables prises en compte dans ce processus décisionnel comprennent les coûts de transaction, les niveaux d'examen réglementaire dans l'ensemble des juridictions et la faisabilité opérationnelle de stratagèmes à plusieurs niveaux impliquant des classes d'actifs dont les processus d'évaluation sont opaques. Pour les acteurs du financement du terrorisme, la prise de décision rationnelle se manifeste par l'exploitation des canaux légitimes disponibles qui comportent de faibles indices de suspicion, limitant ainsi les perturbations de leurs flux de financement. Les objectifs divergents entre l'apprentissage automatique et le financement du terrorisme, à savoir la génération de profits et la fourniture idéologique de ressources, modifient le calcul des avantages perçus, mais présentent des similitudes structurelles dans les stratégies d'évitement des coûts. Le principe de la maximisation de l'utilité dans des conditions de ressources limitées explique pourquoi les deux typologies criminelles exploitent souvent les infrastructures existantes plutôt que de créer des systèmes entièrement nouveaux pour le transfert de fonds. Cela est particulièrement évident dans les réseaux terroristes qui s'approprient des services de transfert de fonds conventionnels ou des organisations caritatives pour acheminer secrètement des fonds (Ryder, n.d.). En utilisant des mécanismes légitimes déjà ancrés dans les systèmes économiques, les auteurs évitent l'investissement substantiel de temps et de capital nécessaire à la conception d'outils alternatifs tout en obtenant le manteau protecteur de la normalité autour de leurs transactions. Pour opérationnaliser la théorie du choix rationnel dans les cadres de LBC/FT, il est essentiel d'identifier comment les mécanismes de dissuasion interagissent avec les calculs des délinquants. Si la probabilité de détection est perçue comme élevée en raison de techniques de surveillance avancées, telles que la détection d'anomalies pilotée par l'IA, les acteurs peuvent recalibrer leurs méthodes ou réorienter l'activité vers des secteurs moins réglementés (Palakurti, 2023). À l'inverse, lorsqu'il existe des lacunes dans l'application de la loi ou la surveillance de la conformité, les modèles rationnels des délinquants prévoient une exploitation accrue de ces faiblesses au fil du temps. La persistance de défaillances stratégiques dans les régimes de lutte contre le blanchiment d'argent de certaines juridictions renforce ce point ; en l'absence de succès visible dans l'application de la loi, les contrevenants potentiels en déduisent que la structure des gains reste favorable aux comportements illicites (Akinteye et coll., 2023). La théorie du choix rationnel aide également à expliquer les modèles d'innovation dans les crimes financiers. Plutôt que d'innover uniquement pour la nouveauté, les criminels adaptent souvent les pratiques existantes pour exploiter les opportunités émergentes ou atténuer les menaces situationnelles, un phénomène décrit comme l'innovation par l'appropriation (Ryder, n.d.). Par exemple, lorsque des réglementations plus strictes réduisent l'attrait des dépôts en espèces de grande valeur, les blanchisseurs peuvent se tourner vers des systèmes basés sur le commerce qui permettent un transfert de valeur équivalente sous un contrôle réduit. Dans les contextes de FTF, l'évolution du climat géopolitique et l'amélioration de la surveillance peuvent inciter à l'adoption

de transferts dispersés de faible valeur qui passent en dessous des seuils algorithmiques. L'application de ce modèle dans des contextes institutionnels tels que BGFIBANK Congo implique d'évaluer comment des mesures de dissuasion ciblées peuvent modifier les analyses coûts-avantages des délinquants. Le renforcement des capacités d'audit interne augmente l'aspect risque de l'équation en améliorant les taux de découverte des contrôles et en assurant des évaluations continues de la conformité (Akinteye et al., 2023). De plus, l'intégration de l'analyse comportementale dans les systèmes de surveillance des transactions crée des barrières dynamiques contre l'exploitation en détectant les écarts par rapport aux normes individuelles des clients plutôt que de s'appuyer exclusivement sur des signaux d'alarme statiques (Paul et al., 2023). De telles mesures augmentent non seulement la probabilité de détection brute, mais aussi l'imprévisibilité perçue du point de vue de l'acteur, un facteur psychologique critique influençant la prise de décision. Une dimension importante de la théorie du choix rationnel est la prise en compte de la rationalité limitée : les contraintes de connaissance, la capacité de traitement cognitif et l'accès à l'information complète affectent les décisions des délinquants tout comme elles le font pour les organismes de réglementation. Les acteurs criminels peuvent surestimer certaines menaces à l'application de la loi ou en sous-estimer d'autres en fonction d'expériences antérieures ou de renseignements incomplets. Cette évaluation imparfaite peut créer des fenêtres exploitables pour des perturbations proactives si les organismes d'application de la loi amplifient stratégiquement les risques perçus au moyen de mesures d'application de la loi publiées ou d'avis ciblés de l'industrie mettant en évidence les vulnérabilités corrigées. De plus, les structures de criminalité en réseau font appel à une rationalité collective, où les processus décisionnels de groupe tiennent compte des ressources partagées et de la tolérance au risque distribuée. Dans de tels arrangements, même si les membres individuels perçoivent défavorablement les risques accrus, la pression du groupe ou la priorisation stratégique par la direction peuvent soutenir les opérations jusqu'à ce que l'impact de l'application de la loi devienne directement tangible pour les nœuds critiques. Cette dynamique souligne la valeur de l'analyse des réseaux sociaux pour isoler les rôles clés des influenceurs au sein des chaînes de blanchiment ou de financement, dont la suppression remodèle les résultats coûts-avantages globaux pour les participants au réseau. D'un point de vue politique, l'intégration de la théorie du choix rationnel dans la conception des programmes de LBC/FT signifie calibrer les interventions de manière que chaque voie potentielle disponible pour un délinquant présente des rendements diminués par rapport aux risques encourus. Cela peut se faire par le biais de plusieurs stratégies :

1. Accroître la certitude et la rapidité de la détection grâce à des mises à niveau technologiques continues associées à une surveillance humaine qualifiée.

2. Élargir l'échange de renseignements intersectoriels afin que les délinquants ne puissent pas facilement migrer leurs activités entre les établissements ou les industries sans être confrontés à des contrôles comparables (LAPTEş, 2023).

3. Resserrement de la couverture réglementaire des secteurs financiers non bancaires traditionnellement considérés comme des cibles faciles en raison de l'allègement de la surveillance.

Chaque mesure modifie les attentes des délinquants en ce qui a trait à la faisabilité opérationnelle et aux gains viables découlant d'activités illégales. Au fil du temps, des changements persistants dans ces attentes réalignent les calculs rationnels vers l'abstention ou l'abandon, un point final théorique aligné sur les cadres de dissuasion intégrés dans les systèmes de justice pénale à l'échelle mondiale. En interprétant les comportements de ML et de TF à travers cette optique, les analystes permettent non seulement de mieux anticiper l'adaptation des méthodes, mais aussi d'élaborer des modèles d'intervention plus proactifs qui manipulent les perceptions des délinquants avant le début des phases d'exécution. Pour des institutions telles que BGFIBANK Congo, qui opèrent dans des environnements

sensibles aux deux typologies de criminalité économique identifiées précédemment, l'intégration de cette compréhension théorique dans les architectures de surveillance fournit aux équipes de conformité une logique prédictive guidant à la fois la hiérarchisation des cas et les décisions d'amélioration du système fondées sur la modification des équilibres coûts-avantages de l'adversaire plutôt que sur la simple réaction à un événement post-transactionnel.

b. Théorie du principal-agent et questions de gouvernance

La théorie du mandant-agent fournit un cadre important pour interpréter les défis de gouvernance qui se posent dans les systèmes de lutte contre le blanchiment d'argent (AML) et le financement du terrorisme (CTF) au sein des institutions financières. À la base, cette théorie examine la relation où un mandant, tel que le conseil d'administration d'une banque ou une autorité de réglementation, délègue des responsabilités opérationnelles à des agents, à savoir des équipes de direction ou des responsables de la conformité. La principale complication est le désalignement potentiel des intérêts entre ces parties. Les agents peuvent poursuivre des objectifs différents de ceux du mandant, en particulier lorsque leurs incitations privilégient la génération de profits à court terme ou la minimisation des coûts plutôt que le strict respect des protocoles AML/CTF. Ce décalage peut se manifester par un sous-investissement dans l'infrastructure de conformité, une adoption superficielle de politiques sans mise en œuvre significative ou un mépris des avertissements externes. Les défaillances des cadres de surveillance et de contrôle illustrent comment l'asymétrie de l'information exacerbe les problèmes des organismes. Les agents détiennent souvent des connaissances opérationnelles plus granulaires que les directeurs, ce qui leur permet de masquer les lacunes dans les contrôles des risques ou de minimiser les alertes qui pourraient signaler des défaillances systémiques. Dans des affaires de lutte contre le blanchiment d'argent très médiatisées, telles que la transaction avec la succursale estonienne de Danske Bank, les enquêtes publiques ont révélé que, bien que toutes les politiques et structures de gestion des risques requises aient été documentées, l'exécution a été inefficace, caractérisée par des défaillances dans les trois lignes de défense (McConnell, 2020). Ces défaillances n'étaient pas simplement des erreurs techniques, mais plutôt des lacunes de gouvernance où les agents n'ont pas agi en conformité avec les objectifs de conformité déclarés par le mandant. Le défi ici est directement lié à la surveillance des coûts et aux mécanismes d'application ; À moins que les directeurs n'auditent et ne valident régulièrement l'activité des agents par des canaux indépendants, il y a peu de dissuasion contre la non-conformité stratégique. Le problème s'aggrave lorsque des opérations internationales complexes se recoupent avec des normes d'application différentes selon les juridictions. Les institutions financières opérant dans des régions où le climat réglementaire est plus faible sont confrontées à des risques accrus si la direction de ces marchés privilégie la croissance des activités locales plutôt que les mandats de conformité à l'échelle du groupe. Les agents peuvent rationaliser les écarts en raison de la faible probabilité perçue de détection ou de sanctions, en exploitant à la fois la distance géographique et organisationnelle par rapport à la surveillance du siège social (Akinteye et al., 2023). La faible capacité de vérification interne aggrave ces risques en réduisant la probabilité que les lacunes soient découvertes et communiquées aux directeurs principaux responsables de la prise de décisions ayant le pouvoir d'intervenir efficacement. La mauvaise gouvernance s'auto-renforce lorsque les précédents de la culture institutionnelle signalent une tolérance à l'égard des manquements à la conformité. Les données suggèrent que le fait de ne pas tenir compte des plaintes externes ou de ne pas mettre à jour les réglementations obsolètes, deux caractéristiques que l'on retrouve dans certains grands scandales de lutte contre le blanchiment d'argent, érode à la fois la perception des employés de l'importance de la politique et l'adhésion réelle (McConnell, 2020). Dans un tel contexte, les gestionnaires du risque opérationnel peuvent se conformer officiellement en tenant à jour la documentation des politiques, mais éviter d'engager les dépenses nécessaires à la surveillance de fond ou aux mesures correctives. Cela reflète un coût d'agence où l'adhésion superficielle satisfait à un examen immédiat tout en masquant les vulnérabilités latentes. Des problèmes d'agence surgissent également lorsque les mesures de performance utilisées pour l'évaluation de la gestion entrent en conflit avec de solides résultats en matière de conformité. Si les structures de bonus récompensent l'acquisition rapide de clients ou le volume de transactions sans tenir compte de manière adéquate des violations de la conformité ou des signalements de risque trop lents, alors le

comportement rationnel des agents penchera vers des activités centrées sur les revenus au détriment de la diligence CTF/AML. Il est donc essentiel d'aligner les systèmes d'incitation sur les priorités de gouvernance pour s'assurer que les agents internalisent les principaux objectifs non seulement au niveau rhétorique, mais aussi dans la prise de décision quotidienne. Les mécanismes pour remédier à ces désalignements comprennent la réduction de l'asymétrie d'information et l'amélioration des structures de responsabilisation afin que les agents agissent conformément aux objectifs de gouvernance dirigés par les directeurs. Les audits internes indépendants réguliers ont un double rôle : ils fournissent des évaluations de performance précises directement aux mandants sans s'appuyer uniquement sur les rapports fournis par les agents, et ils créent une perception permanente parmi les agents que les écarts sont susceptibles d'être découverts. De plus, l'intégration de solides protections des lanceurs d'alerte permet aux acteurs internes au-delà des lignes de signalement formelles d'alerter les dirigeants des irrégularités à des niveaux opérationnels où les audits traditionnels pourraient avoir une portée limitée. Les cadres réglementaires façonnent également la dynamique mandant-agent en imposant des obligations légales aux deux rôles, renforçant ainsi l'influence du mandant sur les agents. Des instruments tels que les lignes directrices nationales en matière de surveillance exigent que les unités d'audit interne fonctionnent de manière indépendante de la direction et imposent des ressources adéquates pour les fonctions de conformité (Akinteye et al., 2023). Des organismes internationaux comme le GAFI renforcent ces exigences par des recommandations préconisant des processus d'assurance indépendants comme moyen de vérifier l'efficacité des contrôles LBC/FT. Cependant, les stratégies d'amélioration de la conformité doivent tenir compte de la résistance potentielle des agents confrontés à des exigences de surveillance accrues. La théorie de la gouvernance indique que si l'on ne cultive pas une culture alignée sur la conduite éthique et la transparence, une surveillance supplémentaire peut produire des comportements de dissimulation plutôt qu'un véritable changement de comportement. Par exemple, le traçage basé sur la blockchain pourrait améliorer la transparence des réseaux transactionnels (Ji, 2023), mais son potentiel pourrait être sapé si les gestionnaires locaux le perçoivent principalement comme une surveillance destinée à discipliner plutôt qu'à soutenir l'intégrité opérationnelle. L'intégration de la technologie offre des possibilités d'atténuer les conflits d'agence en réduisant le recours à l'interprétation subjective des anomalies de transaction par les agents. Les plateformes d'analyse avancées qui s'appuient sur l'apprentissage automatique peuvent normaliser les seuils de détection entre les succursales, indépendamment de la discrétion de la direction locale, tout en générant des pistes d'audit accessibles directement par les directeurs (Palakurti, 2023). Le signalement automatisé réduit la dépendance vis-à-vis des décisions d'escalade initiées par l'agent, qui sont susceptibles d'être prises en cas de conflits d'intérêts ou d'ignorance volontaire. Dans le même temps, la gouvernance reste indispensable car même les systèmes avancés nécessitent une configuration correcte et une action de suivi sur les alertes générées, un processus toujours sous contrôle managérial (Ji, 2023). Ainsi, la technologie devrait compléter, mais non remplacer, les régimes de gouvernance ancrés dans des chaînes de responsabilisation claire reliant directement les actions de première ligne aux mandats principaux. En fin de compte, l'application de la théorie du mandant-agent souligne qu'une gouvernance efficace de la lutte contre le blanchiment d'argent et le financement du terrorisme dépend de la gestion active de cette relation contractuelle dans des conditions d'information imparfaite et d'incitations divergentes. Pour minimiser les coûts d'agence, il faut structurer les politiques organisationnelles de manière à ce que les motivations des agents s'alignent naturellement sur les objectifs réglementaires grâce à un recalibrage des incitations, à des processus d'amélioration de la transparence, à des structures d'audit indépendantes rigoureuses et à des niveaux de normalisation technologique qui limitent la suppression discrétionnaire des alertes (Eijkman, 2013). L'incapacité à s'attaquer à ces problèmes laisse des vulnérabilités systémiques ouvertes où les décisions individuelles éclairées par l'intérêt personnel peuvent s'agréger en une exposition à l'échelle de l'institution, menaçant non seulement la position réglementaire, mais aussi l'intégrité du système financier en général.

c. Perspectives criminologiques sur le blanchiment d'argent et le financement du terrorisme

Les analyses criminologiques du blanchiment d'argent et du financement des activités terroristes vont au-delà des mécanismes transactionnels pour prendre en compte les facteurs sociaux, psychologiques et structurels plus larges qui influencent ces activités. L'une des principales perspectives examine comment

les réseaux du crime organisé et les organisations terroristes adaptent leurs comportements financiers de manière à répondre directement aux pressions réglementaires, aux environnements d'application de la loi et aux vulnérabilités perçues du système financier. De ce point de vue, les mesures préventives visant uniquement à réprimer la dissimulation de fonds illicites peuvent être insuffisantes si elles négligent les facteurs qui sous-tendent la commission d'infractions sous-jacentes elles-mêmes. Si les entreprises criminelles sous-jacentes telles que le trafic de drogue ou la corruption restent viables et rentables, les activités de blanchiment en aval risquent de persister malgré le renforcement des sanctions contre les actes de blanchiment de passes. Le rôle de la théorie de la dissuasion dans la criminologie recoupe ici les principes du choix rationnel discutés précédemment à la section 2.2.1. La dissuasion repose sur la perception qu'ont les délinquants potentiels que l'appréhension est à la fois probable et conséquente ; Cependant, les études criminologiques suggèrent que ces perceptions sont influencées par les conditions socioéconomiques, la culture organisationnelle au sein des groupes criminels et les antécédents en matière d'application de la loi dans une administration donnée. Par exemple, lorsque les organismes de lutte contre le blanchiment d'argent promeuvent des discours selon lesquels les fonds blanchis seront inévitablement saisis et confisqués, les acteurs peuvent changer de méthode, mais ne pas abandonner complètement les opérations s'ils jugent que les taux de réussite réels de l'application de la loi sont faibles (de Araújo, 2012). Ce décalage entre les messages formels et les résultats tangibles de l'application de la loi met en évidence une préoccupation criminologique : les lois symboliques sans impact démontrable risquent de favoriser le cynisme plutôt que la conformité. Du point de vue de l'interprétation fonctionnaliste appliquée aux crimes financiers, les processus judiciaires jouent un rôle tout aussi important que les cadres législatifs dans l'élaboration de normes contre le blanchiment d'argent et le financement du terrorisme. Les tribunaux qui interprètent des infractions impliquant des instruments financiers émis en violation de la réglementation adoptent souvent une lentille téléologique, donnant la priorité aux objectifs de niveau sociétal tels que le maintien de la stabilité du marché plutôt qu'aux détails techniques de procédure dans la définition de la culpabilité (Fu et al., 2024). Cette orientation reflète une reconnaissance sociologique selon laquelle la protection de la confiance systémique dans le système financier est aussi essentielle que la poursuite des délinquants individuels. Le personnel interne qui abuse de l'accès pour émettre des instruments à des fins illégales ne se contente pas de violer des dispositions légales distinctes ; Ils déstabilisent l'ordre normatif au sein des échanges économiques. De tels actes nécessitent des réponses équilibrant des actions punitives et des réformes préventives ciblant les vulnérabilités institutionnelles exploitées par des initiés. Les modèles criminologiques mettent également l'accent sur les dimensions relationnelles du financement illicite. Les acteurs du blanchiment de capitaux ou du financement du terrorisme opèrent rarement de manière isolée ; ils fonctionnent plutôt au sein de réseaux caractérisés par des mécanismes de confiance, des normes de réciprocité et des stratégies partagées d'atténuation des risques (Godefroy et coll., 2011). Ces liens sociaux facilitent la sécurité opérationnelle en créant des canaux d'échange d'informations en dehors des systèmes formels, communément appelés « échanges d'informations » entre des parties situées à différents points des chaînes de blanchiment ou de financement. Dans certains cas, les acteurs établissent des alliances informelles avec des employés légitimes du secteur prêts à partager des renseignements internes. Pour comprendre ces interactions d'un point de vue criminologique, il faut examiner non seulement les motivations économiques, mais aussi l'ancrage de ces crimes dans des contextes sociopolitiques plus larges où les frontières floues entre les acteurs licites et illicites contribuent à la persistance malgré les contraintes réglementaires. Les progrès technologiques introduisent d'autres considérations criminogènes. Alors que les analyses basées sur l'IA sont de plus en plus intégrées aux régimes de lutte contre le blanchiment d'argent et le financement du terrorisme pour la détection précoce (Palakurti, 2023), les criminels font preuve de capacités d'adaptation en déplaçant leur empreinte opérationnelle vers des plateformes moins surveillées lorsqu'ils font l'objet d'une surveillance accrue. Cet effet de déplacement s'aligne sur la théorie criminologique du déplacement : les interventions ciblant un modus operandi peuvent déplacer la criminalité vers d'autres lieux à moins qu'une couverture systémique ne soit assurée par des canaux interconnectés. Par exemple, une surveillance accrue des virements bancaires peut inciter à recourir davantage à des systèmes de blanchiment commercial ou à des transactions décentralisées en monnaie numérique qui manquent d'une rigueur de surveillance équivalente. Par conséquent, du point de vue de la prévention, les architectures de surveillance dynamique doivent évoluer en même temps que les cycles d'adaptation des délinquants plutôt que de supposer que les typologies statiques resteront prédominantes au fil du temps. Un autre aspect mis en

évidence par la criminologie concerne les structures d'opportunité permettant l'innovation en matière de blanchiment d'argent et de financement du terrorisme, en particulier dans des conditions socioéconomiques changeantes telles que celles provoquées par des crises mondiales comme la COVID-19 (Ryder, n.d.). Les perturbations des flux économiques conventionnels créent à la fois des angles morts dans les routines d'application de la loi et de nouvelles échappatoires exploitables pour les mouvements illicites de fonds. L'analyse comparative des innovations financières parmi les start-ups donne un aperçu de la capacité d'adaptation entrepreneuriale similaire observée chez les financiers du terrorisme qui mobilisent des ressources de manière créative dans des environnements riches en contraintes. En situant les stratégies de BA/FAT dans les cadres de la théorie des opportunités, où l'exposition à des opportunités criminelles viables interagit avec la préparation des délinquants, les chercheurs peuvent mieux anticiper les changements dans les méthodes de blanchiment ou de financement préférées lors de bouleversements sociopolitiques ou de transitions de marché. Les criminologues se concentrent également sur les défaillances de la gouvernance en tant que facteurs facilitateurs de la persistance du BA/FAT. La faiblesse des systèmes de contrôle au sein des institutions laisse la possibilité aux individus agissant en tant qu'agents d'exploiter les avantages asymétriques en matière de connaissances par rapport aux directeurs chargés de la surveillance (McConnell, 2020). Lorsque les cultures de conformité tolèrent des écarts mineurs par rapport aux protocoles établis en raison de pressions concurrentielles ou de priorités en matière de coûts, l'érosion cumulative des normes peut entraîner une exposition substantielle au fil du temps. Ces défaillances de gouvernance entrent en résonance avec les théories abordant la dynamique de la criminalité en col blanc : les auteurs rationalisent souvent leurs actions par le déni du préjudice ou la diffusion de la responsabilité, tout en bénéficiant de l'impunité perçue offerte par l'isolement organisationnel des récits de victimisation publique directe. Les approches préventives préconisées en criminologie mettent donc l'accent sur des interventions à plusieurs niveaux combinant certitude punitive et restructuration environnementale pour réduire les possibilités de commission de crimes. Il s'agit notamment d'améliorer les mécanismes de coopération interorganismes afin que les renseignements relatifs aux typologies émergentes soient partagés en temps opportun entre les organismes d'application de la loi, les organismes de réglementation et les intervenants du secteur privé (Godefroy et coll., 2011). Une telle collaboration reflète la théorie de la prévention situationnelle de la criminalité appliquée dans des contextes financiers : la modification des variables situationnelles, comme l'augmentation de l'effort requis pour les délinquants par des procédures KYC plus strictes ou la réduction des incitations par des politiques de confiscation des biens, peut perturber les infractions planifiées sans nécessiter de transformation de la moralité des délinquants. Enfin, des considérations éthiques émergent lorsque les mesures de lutte contre la criminalité recoupent les protections des libertés civiles, un thème récurrent dans le discours sur la lutte contre le financement du terrorisme (Ryder, n.d.). La criminologie critique les approches de surveillance trop larges qui érodent la vie privée sans gains proportionnels en matière d'efficacité de l'interdiction ; Ceux-ci peuvent miner par inadvertance la légitimité des régimes de réglementation s'ils sont perçus comme oppressifs plutôt que protecteurs. Le maintien de cet équilibre exige une justification transparente des tactiques intrusives fondées sur des résultats démontrables d'atténuation des risques plutôt que sur des préjudices spéculatifs seuls. Dans des contextes tels que l'environnement opérationnel de BGFIBANK Congo, où les défis de gouvernance se recoupent avec les instabilités socio-économiques régionales, l'application de ces connaissances criminologiques équilibrées soutient l'élaboration de systèmes de LBC/FT réactifs à la fois à la dynamique des risques contextuels et aux attentes sociétales plus larges en matière d'équité et de préservation des droits, tout en soutenant la dissuasion opérationnelle contre les adversaires adaptatifs dans les spectres du ML et du FFAT.

6. Risques et impacts pour les institutions bancaires

Les institutions bancaires sont en première ligne face aux risques générés par les activités illicites telles que le blanchiment de capitaux, le financement du terrorisme (FT) et la fraude financière. Ces phénomènes exposent les banques à une palette de risques multiples, dont les effets peuvent être cumulatifs, systémiques et dévastateurs à long terme.

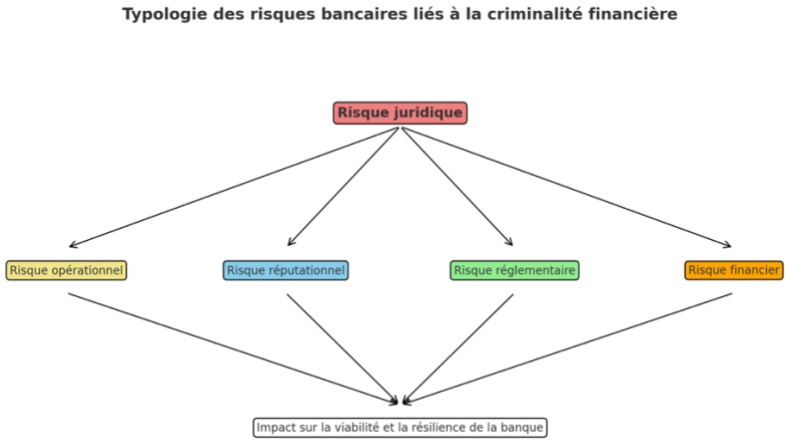
Premièrement, le **risque juridique** découle directement de la non-conformité réglementaire. Une banque qui facilite, même involontairement, le passage de fonds illicites ou le financement d'activités terroristes s'expose à des sanctions administratives, des amendes colossales, voire des poursuites pénales. À titre d'exemple, la banque britannique HSBC a écopé en 2012 d'une amende de 1,9 milliard de dollars pour des manquements dans ses dispositifs LCB-FT (*FATF, 2022*). En zone CEMAC, la COBAC peut suspendre un établissement ou révoquer ses dirigeants en cas de violation grave des normes de lutte contre la criminalité financière (*COBAC, 2023*).

Deuxièmement, les institutions sont confrontées à un **risque réputationnel**, difficilement quantifiable mais extrêmement préjudiciable. Une fois impliquée dans un scandale de blanchiment ou de financement du terrorisme, une banque peut voir sa crédibilité entachée, sa clientèle se détourner et ses partenaires internationaux limiter ou suspendre leurs relations. Dans une économie mondialisée, la réputation devient un actif stratégique intangible, déterminant pour l'accès aux marchés de capitaux (*Basel Committee, 2016*).

Le **risque opérationnel** est aussi une conséquence majeure. Il provient du manque de contrôle interne, de défaillances humaines ou technologiques, facilitant la fraude ou l'infiltration de flux illicites. Ces vulnérabilités pèsent sur la résilience organisationnelle et révèlent des failles dans les systèmes d'information, les procédures d'ouverture de comptes, ou encore la segmentation des droits d'accès (*ACFE, 2022*).

À cela s'ajoute un **risque financier direct**, lié aux pertes enregistrées (dans les cas de fraude interne, détournement ou remboursement d'opérations frauduleuses), mais aussi indirect (coûts d'investigation, mise à jour des systèmes, audits de conformité, etc.).

Enfin, le **risque réglementaire**, de plus en plus central, provient de la pression croissante des autorités de supervision, des standards internationaux (FATF, Basel III) et des obligations nationales (Loi CEMAC, FATCA, AMLD 5 dans l'UE).



Matrice des risques bancaires et des impacts liés à la criminalité financière

Tableau 2: risques et des impacts liés à la criminalité financière

Type de risque	Définition	Exemples	Impacts potentiels

Risque juridique	Responsabilité légale pour manquement aux normes LCB-FT	Amendes, révocation de licence (ex: HSBC 2012)	Procédures judiciaires, perte de licence d'exploitation
Risque réputationnel	Atteinte à l'image ou à la crédibilité institutionnelle	Perte de partenaires, réputation médiatique négative	Fuite des clients, baisse de valorisation boursière
Risque opérationnel	Défaillance des processus, systèmes ou ressources humaines	Ouverture de compte frauduleux, système d'alerte inopérant	Blocage des opérations, augmentation des coûts internes
Risque financier	Pertes directes ou coûts induits liés à la criminalité financière	Vol interne, remboursement d'opérations frauduleuses	Baisse de rentabilité, provisionnement accru
Risque réglementaire	Sanctions ou restrictions liées à la non-conformité	Non-respect des obligations FATF, COBAC ou FATCA	Suspension d'activités, limitation des partenariats

Face à ces risques multiples, les banques doivent développer une vision holistique de la conformité, intégrant à la fois technologies de surveillance, gouvernance renforcée et culture du risque. L'enjeu dépasse la simple conformité réglementaire : il s'agit de protéger la confiance, la stabilité et la légitimité du système bancaire, dans un contexte international de plus en plus exigeant.

Ce premier chapitre a permis de cadrer les concepts centraux et les typologies d'opérations liées au blanchiment de capitaux et au financement du terrorisme. Il montre que les enjeux vont bien au-delà du respect réglementaire : il s'agit d'une véritable lutte pour la résilience et la réputation du système bancaire, dans un environnement complexe et en mutation. Cette compréhension permettra d'aborder, dans le chapitre suivant, les cadres réglementaires et institutionnels qui encadrent la lutte contre ces phénomènes.

Chapitre 2 – Cadres réglementaires et institutionnels mondiales et régionales en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme

Le blanchiment de capitaux et le financement du terrorisme (BC/FT) constituent aujourd'hui deux des menaces les plus sérieuses pour la stabilité financière mondiale, la sécurité des États et la confiance des acteurs économiques. Face à la multiplication des opérations frauduleuses et à leur sophistication croissante, les réponses juridiques et institutionnelles se sont progressivement renforcées, dessinant un cadre normatif dense et multiforme. Ce dispositif repose sur une articulation entre initiatives internationales, régionales et nationales, dont la cohérence et l'efficacité conditionnent directement la capacité des institutions bancaires à identifier, prévenir et sanctionner les comportements illicites.

Au niveau international, les normes édictées par le Groupe d'action financière (GAFI) constituent le socle de la régulation mondiale. Leurs quarante recommandations, régulièrement actualisées, fixent les standards de vigilance, de coopération et de transparence applicables à l'ensemble des pays membres et partenaires. Ces prescriptions sont relayées et complétées par d'autres organisations telles que l'Office des Nations Unies contre la drogue et le crime (ONUDC) ou le Comité de Bâle, qui apportent une expertise technique et des directives spécifiques aux institutions financières.

Dans l'espace africain, des instances régionales telles que la CEMAC, à travers la Commission bancaire d'Afrique centrale (COBAC), jouent un rôle central dans l'adaptation de ces normes aux réalités locales. Le cadre national, notamment en République du Congo, traduit ces exigences en obligations contraignantes pour les établissements bancaires, sous le contrôle d'organismes spécialisés comme l'Agence nationale d'investigation financière (ANIF).

Enfin, l'examen comparatif avec d'autres juridictions, qu'elles soient africaines ou internationales, permet de mettre en évidence les écarts, les bonnes pratiques et les défis persistants. Ce chapitre propose donc une analyse détaillée de ces différents niveaux d'encadrement, tout en soulignant leurs implications pratiques pour une institution comme BGFIBANK Congo, appelée à conjuguer conformité réglementaire, performance opérationnelle et gestion stratégique des risques.

1. Les Cadres réglementaires et Normes Internationales de lutte contre le blanchiment de capitaux et le financement du terrorisme

L'architecture mondiale de la lutte contre le blanchiment d'argent et le financement du terrorisme (LBC/FT) repose sur une combinaison de normes internationales, de dispositifs juridiques, de mécanismes d'évaluation et de collaboration interinstitutionnelle. Elle vise à doter les juridictions nationales de cadres robustes et adaptatifs pour répondre aux dynamiques de la criminalité financière. Le Groupe d'action financière (GAFI) en constitue le pilier central. Créé en 1989, il a étendu son champ d'intervention initialement centré sur les flux liés au trafic de drogue pour inclure le financement du terrorisme, de la prolifération des armes, la corruption, et plus largement toutes les formes émergentes de criminalité financière (Helgesson & Mörth, 2018 ; Godefroy et al., 2011).

a. Recommandations du Groupe d'action financière (GAFI)

Le GAFI a établi 40 recommandations qui forment une référence mondialement reconnue, articulant des mesures préventives, répressives, de coopération internationale, et des exigences applicables aux banques, aux institutions financières non bancaires, ainsi qu'aux entreprises et professions non

financières désignées (EPNFD). Ces recommandations sont dotées d'un mécanisme d'évaluation mutuelle, qui analyse tant la conformité technique que l'efficacité opérationnelle des dispositifs nationaux (Akinteye et al., 2023). Ce mécanisme de revue par les pairs est particulièrement influent, puisque les juridictions dont les dispositifs sont jugés déficients peuvent être inscrites sur la « liste grise » ou la « liste noire » du GAFI, restreignant leur accès aux marchés financiers internationaux, et exerçant ainsi une pression macroéconomique (Ryder, s.d.). Un principe fondamental du cadre du GAFI est l'approche fondée sur les risques. Elle invite les États et les entités assujetties, comme les banques, à allouer les ressources de manière proportionnée aux secteurs et produits les plus vulnérables (Ryder, n.d.). Cela contraste avec une application uniforme des contrôles, et suppose une capacité d'évaluation dynamique, tenant compte de la typologie du client, des zones géographiques concernées, de la complexité des produits financiers, et des canaux de distribution. Dans les juridictions à haut risque comme la République démocratique du Congo (RDC), cela implique une segmentation granulaire des clients et un recalibrage continu des profils de risques (Akinteye et al., 2023). Les recommandations 5, 6, 10, 13 et 20 du GAFI sont particulièrement structurantes. La recommandation 10 impose des procédures rigoureuses de vigilance à l'égard de la clientèle (CDD), incluant l'identification des bénéficiaires effectifs, la vérification des informations fournies, et un contrôle continu des opérations (Utkina et al., 2023). La recommandation 20 exige de signaler toute opération suspecte, indépendamment de son exécution, sans en avertir le client, pour éviter d'entraver les enquêtes (Palakurti, 2023). En parallèle, la recommandation 6 impose l'application immédiate de sanctions financières issues des résolutions du Conseil de sécurité de l'ONU, notamment les résolutions 1267 et 1373 relatives à la lutte contre le terrorisme (Ryder, s.d.). La recommandation 13 concerne les relations interbancaires transfrontalières, notamment la diligence renforcée à l'égard des banques correspondantes dans des juridictions exposées. Ces prescriptions visent à prévenir l'exposition indirecte à des flux illicites, en analysant les structures de propriété, la gouvernance, ou la réputation réglementaire (Helgesson & Mörth, 2018). Les avancées technologiques sont intégrées dans l'approche du GAFI. Celui-ci encourage l'adoption d'outils d'intelligence artificielle pour la surveillance transactionnelle, à condition qu'ils soient transparents, auditables et validés empiriquement (Palakurti, 2023). Le traitement des actifs numériques et l'activité des prestataires de services de cryptoactifs sont également soumis aux obligations LBC/FT, notamment via les notes interprétatives révisées. Le Comité de Bâle sur le contrôle bancaire (CBCB) vient renforcer la mise en œuvre opérationnelle de ces normes. Il traduit les objectifs stratégiques du GAFI en exigences prudentielles détaillées intégrées aux structures de gouvernance, aux systèmes de gestion des risques et aux contrôles internes bancaires. L'une de ses contributions majeures est la redéfinition de la vigilance client non plus comme une exigence réglementaire isolée, mais comme un élément clé de la gestion globale des risques, au même titre que l'évaluation du risque de crédit ou de marché (Utkina et al., 2023). Il recommande l'élaboration de politiques différenciées en fonction du profil de risque du client, approuvées au niveau du conseil d'administration. Dans ce cadre, les institutions comme BGFIBANK Congo doivent mettre en place des modèles intégrés de profilage, couplant les résultats de la surveillance continue avec des mécanismes de recalibrage automatique du risque. Les systèmes d'alerte doivent être dynamiques, capables de détecter les changements comportementaux, comme les transferts transfrontaliers soudains en provenance de zones à risque, et de déclencher une reclassification immédiate du client (Palakurti, 2023).

b. Lignes directrices du Comité de Bâle

Le Comité de Bâle sur le contrôle bancaire (CBCB) a progressivement intégré dans ses lignes directrices des dispositions influençant les cadres de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT). Ces orientations traduisent des objectifs stratégiques globaux en principes prudentiels relatifs à la gouvernance, la gestion des risques et les dispositifs de contrôle (Akinteye et al., 2023). Elles intègrent la LBC/FT dans les systèmes de gestion du risque opérationnel, dépassant une vision cloisonnée. Un pilier majeur est la vigilance à l'égard de la clientèle (CDD), élevée au rang d'élément central de la gestion bancaire (Utkina et al., 2023). Cette vigilance est liée à des politiques d'acceptation différenciées selon les profils de risque. Pour des institutions comme BGFIBANK Congo, cela suppose des méthodologies documentées afin d'adapter les mesures de diligence à l'activité, à l'exposition géographique et à la complexité des canaux. Le CBCB insiste sur une surveillance continue

intégrant une boucle de rétroaction entre les comportements observés et la réévaluation des seuils de détection. Ainsi, les changements dans les schémas de transaction liés à des zones sensibles doivent réviser en temps réel les profils de risque, renforçant la pertinence des alertes. Ces pratiques rejoignent les recommandations d'intégration d'outils d'IA et de machine learning pour extraire des anomalies complexes (Palakurti, 2023).

La gouvernance est au cœur des recommandations. Le conseil d'administration est responsable de politiques cohérentes et dotées de ressources, y compris pour les filiales à l'étranger (McConnell, 2020). La haute direction doit assurer leur diffusion et favoriser la remontée d'informations sans crainte de représailles, tandis que l'audit interne évalue leur efficacité réelle (Helgesson & Mörth, 2018 ; Akinteye et al., 2023). Les conclusions doivent remonter directement au conseil ou à un comité d'audit pour éviter les conflits d'intérêts. Les lignes directrices rappellent aussi l'importance d'une diligence renforcée vis-à-vis des correspondants bancaires. Les institutions doivent vérifier non seulement l'existence, mais aussi l'efficacité des programmes de LBC/FT de leurs partenaires (Helgesson & Mörth, 2018). Dans des régions comme l'Afrique centrale, où l'accès aux correspondants est sensible au risque pays, ces critères deviennent cruciaux (Godefroy et al., 2011). La tenue des documents est considérée comme une garantie de résilience et de preuves suffisantes pour les enquêtes. L'accent est mis sur l'archivage sécurisé et l'interopérabilité des données dans un contexte de numérisation (Akinteye et al., 2023). En parallèle, l'adoption de nouvelles technologies doit s'accompagner de validations rigoureuses, notamment pour les systèmes d'IA, afin d'éviter les « boîtes noires » et les biais (Palakurti, 2023).

Le CBCB encourage par ailleurs la transparence dans les relations avec les superviseurs : divulgation proactive en cas de défaillances, plans de remédiation et coopération transfrontalière (Godefroy et al., 2011). Les lignes directrices lient aussi la LBC/FT à l'appétence globale au risque, demandant que les conseils d'administration fixent des limites claires d'exposition résiduelle, afin d'éviter que la pression commerciale ne compromette la conformité (McConnell, 2020). Des tests de résistance sont recommandés pour évaluer la robustesse des systèmes face à des scénarios atypiques, comme des flux massifs de réfugiés ou des chocs sur les matières premières (Ryder, n.d.). Ces exercices encouragent une coopération entre conformité, sécurité informatique et audit. Enfin, le CBCB soutient la coopération intersectorielle et les partenariats public-privé, promouvant l'intégration des données issues des activités de surveillance dans les typologies sectorielles (Helgesson & Mörth, 2018). Ainsi, les directives du CBCB articulent la LBC/FT comme une composante de la gouvernance bancaire, en insistant sur la vigilance client, la surveillance dynamique, la rigueur documentaire, la validation technologique et la coopération internationale. Pour des banques opérant dans des juridictions à risque élevé comme BGFIBANK Congo, elles représentent à la fois un outil de stabilisation et un levier de crédibilité (Akinteye et al., 2023).

c. Initiatives du Groupe Egmont

Le Groupe Egmont des cellules de renseignement financier (CRF) constitue une pierre angulaire de la lutte mondiale contre le blanchiment de capitaux et le financement du terrorisme (BC/FT). Il offre une plateforme sécurisée de coopération permettant aux CRF de partager renseignements et expertises dans un cadre aligné sur les standards du GAFI (Helgesson & Mörth, 2018). En République démocratique du Congo (RDC), la CRF nationale profite directement de ces mécanismes à travers l'accès à l'Egmont Secure Web (ESW), outil centralisé facilitant l'échange rapide de données sensibles sur des schémas transfrontaliers complexes (Quintel, 2022). Dans des contextes où les exportations minières sont vulnérables à des manipulations de prix, ESW permet de vérifier auprès de pairs étrangers la légitimité des contreparties et de détecter des bénéficiaires effectifs cachés. Les activités d'Egmont ne se limitent pas à la communication. Elles incluent un renforcement des capacités analytiques, notamment via des formations avancées sur l'analyse de réseaux appliquée aux structures opaques de propriété (Godefroy et al., 2011). Ces ateliers, combinés à l'intégration de données non traditionnelles (douanes, registres d'actifs), améliorent les capacités nationales de détection. Pour une institution comme BGFIBANK Congo, la traduction de ces signaux en règles internes renforce la détection dans des secteurs sensibles comme le commerce transfrontalier.

Un autre objectif majeur d'Egmont consiste à améliorer la qualité des renseignements exploitables plutôt que d'accroître le volume des déclarations. Dans de nombreuses économies émergentes, la surdéclaration issue de seuils rigides entraîne une surcharge analytique (Palakurti, 2023). L'assistance technique d'Egmont privilégie donc une approche basée sur le risque, alignée sur le principe de proportionnalité du GAFI, afin que les ressources se concentrent sur les cas les plus menaçants. L'harmonisation juridique fait également partie des priorités : protocoles d'entente bilatéraux et reconnaissance mutuelle des régimes de confidentialité permettent de garantir l'admissibilité des preuves échangées devant les tribunaux (Quintel, 2022). Cette dimension est cruciale pour les gels d'avoirs coordonnés où les flux transitent par plusieurs juridictions. Egmont encourage aussi l'adoption de technologies émergentes. L'usage du Big Data et de l'apprentissage automatique pour classer les déclarations d'activité suspecte illustre cette tendance (Ji, 2023). Ces innovations permettent d'améliorer la rapidité et la pertinence des enquêtes, tout en s'appuyant sur le retour d'expérience international. L'organisation promeut également les partenariats public-privé, qui offrent un cadre sécurisé pour discuter des tendances émergentes de structuration ou des vulnérabilités sectorielles (Godefroy et al., 2011). Pour les banques locales, cela se traduit par un accès indirect à une intelligence mondiale sur les méthodes de BC/FT, telles que l'utilisation abusive des transferts de fonds par des cellules terroristes (Ryder, n.d.).

Enfin, l'adhésion aux normes strictes de confidentialité d'Egmont est un gage de confiance, indispensable pour recevoir des informations sensibles impliquant des personnes politiquement exposées (Quintel, 2022). Dans un pays où certains secteurs stratégiques sont exposés à l'influence d'acteurs connectés (Utkina et al., 2023), la crédibilité internationale dépend de la démonstration de capacités solides et conformes aux standards. D'un point de vue stratégique, la participation active aux travaux d'Egmont améliore les évaluations du GAFI, accroît les résultats opérationnels (gel d'avoirs, poursuites, perturbation de réseaux transnationaux) et facilite le maintien des relations avec les correspondants bancaires essentiels (Helgesson & Mörth, 2018).

En somme, le Groupe Egmont fournit une infrastructure technologique sécurisée, un renforcement des compétences analytiques, des cadres juridiques harmonisés, une intégration de l'innovation technologique et un dialogue structuré avec le secteur privé. Pour la RDC et ses institutions financières, exploiter ces atouts représente une stratégie clé pour combler les lacunes de capacités et s'inscrire dans une architecture internationale conçue pour devancer l'ingéniosité des acteurs du blanchiment et du financement du terrorisme.

2. Cadres réglementaires régionales en Afrique : convergence normative et renforcement institutionnel

Face à l'intensification des flux illicites transnationaux, à la diversification des méthodes de blanchiment de capitaux (BC) et de financement du terrorisme (FT), ainsi qu'à la transformation numérique des systèmes financiers, les pays africains ont progressivement renforcé leurs cadres réglementaires LBC/FT. Cette évolution s'est opérée sous l'impulsion des recommandations du Groupe d'action financière (GAFI) et par le biais de structures régionales telles que le GIABA, l'ESAAMLG, ou le GABAC. En Afrique centrale, la CEMAC constitue un exemple structurant d'intégration des mécanismes de supervision, notamment à travers le rôle central de la COBAC. Toutefois, malgré l'harmonisation normative affichée, les défis juridiques, techniques et opérationnels demeurent considérables, menaçant l'efficacité de la convergence régionale. Ce résumé analyse les logiques d'articulation des normes internationales dans les juridictions africaines, en mettant l'accent sur la supervision régionale en Afrique centrale, les mécanismes de coopération transfrontalière, et les obstacles persistants à une harmonisation opérationnelle. La régionalisation de la lutte contre le blanchiment d'argent en Afrique repose sur l'appropriation des standards internationaux et leur adaptation aux réalités locales. Les cadres réglementaires mis en place dans différentes juridictions africaines s'inscrivent dans un processus de convergence vers les standards du GAFI, tout en tenant compte des spécificités locales telles que la forte prévalence des économies informelles, l'utilisation

intensive de la liquidité, les frontières poreuses ou la faible bancarisation (Helgesson & Mörth, 2018). Des blocs régionaux comme l'ESAAMLG en Afrique de l'Est et australe, ou le GIABA en Afrique de l'Ouest, jouent un rôle structurant en évaluant les dispositifs nationaux, en facilitant la coopération technique, et en promouvant l'analyse des typologies propres à chaque zone. Leurs travaux permettent aux États membres de disposer de feuilles de route adaptées à leur exposition aux risques et de bénéficier de bonnes pratiques adaptées aux défis de chaque région (Godefroy et al., 2011). Sur le plan national, les réformes réglementaires ont été guidées par l'intégration du devoir de vigilance à l'égard de la clientèle (CDD), la transparence sur les bénéficiaires effectifs, la surveillance transactionnelle, et la déclaration systématique des opérations suspectes. En parallèle, les autorités réglementaires ont renforcé les conditions d'agrément des institutions financières, imposant la démonstration préalable de dispositifs LBC/FT crédibles (McConnell, 2020). Les cellules de renseignement financier (CRF) jouent un rôle central dans ce dispositif, en tant que réceptacles des déclarations d'opérations suspectes, mais aussi comme centres d'analyse stratégique. Plusieurs CRF africaines se dotent aujourd'hui de capacités technologiques avancées pour analyser des volumes croissants de données, intégrer des sources non conventionnelles (données douanières, registres de propriété foncière, documents fiscaux), et identifier des typologies propres à des activités criminelles régionales (Kozlova et al., 2023).

a. Le rôle de la COBAC dans la supervision LBC/FT en Afrique centrale

La Commission Bancaire de l'Afrique Centrale (COBAC) est l'organe de supervision prudentielle de la zone CEMAC et constitue le bras armé de l'application des normes LBC/FT dans les six pays membres. Son action s'inscrit dans une double logique : d'une part, transposer les standards du GAFI en les adaptant aux vulnérabilités régionales ; d'autre part, harmoniser les niveaux de conformité malgré les capacités hétérogènes des institutions nationales (Helgesson & Mörth, 2018). Sur le plan normatif, la COBAC émet des textes réglementaires contraignants transposant les recommandations du GAFI, en intégrant les réalités économiques locales comme l'usage prédominant du cash, l'activité informelle ou encore le blanchiment fondé sur le commerce des matières premières (Godefroy et al., 2011). Ces textes couvrent le devoir de vigilance, les mesures renforcées pour les PPE, la conservation des données, la déclaration des opérations douteuses (DOD), et la gouvernance interne. Opérationnellement, la COBAC articule supervision sur site et hors site. Les inspections sur site incluent l'audit des fichiers clients, la revue des systèmes automatisés de détection, ou encore l'analyse des délais de déclaration (Akinteye et al., 2023). La supervision hors site se base sur des rapports statistiques et des indicateurs d'activité synthétiques permettant de repérer les sous-performances. Le COBAC publie également des circulaires sectorielles en réaction à des typologies émergentes transmises par les CRF (Quintel, 2022). Son rôle de coordination est central dans un contexte où les risques de blanchiment et de financement du terrorisme sont transfrontaliers. Le COBAC collabore étroitement avec le GABAC, le régulateur régional de type GAFI, et les CRF nationales, notamment pour la création de typologies régionales, la consolidation de bases de données, ou la coordination des inspections mixtes dans les zones frontalières.

b. Coopération transfrontalière entre les États de la CEMAC : vers une réponse concertée aux menaces régionales

Les mécanismes de coopération entre les États de la CEMAC visent à répondre aux vulnérabilités liées à la porosité des frontières, aux flux commerciaux informels, et à l'interdépendance économique entre pays membres. Cette coopération dépasse l'harmonisation formelle des textes pour inclure des actions opérationnelles, des formations conjointes, des échanges d'informations sensibles, et des inspections coordonnées (Helgesson & Mörth, 2018). Les CRF échangent régulièrement des renseignements via des canaux sécurisés conformes aux standards du Groupe Egmont. Ces échanges portent aussi bien sur les STR que sur des alertes préventives concernant des typologies émergentes, comme les fausses facturations dans le commerce pétrolier ou les dérives de certaines institutions de microfinance proches des frontières (Quintel, 2022). L'effort d'harmonisation passe également par des ateliers conjoints réunissant régulateurs, analystes des CRF et responsables de conformité des banques régionales. Ces forums permettent d'aligner les pratiques de surveillance sur des menaces partagées, telles que les

transferts informels de fonds ou les abus dans le financement du commerce (Godefroy et al., 2011). La coordination des inspections par le COBAC, avec des équipes mixtes d'inspecteurs issus de plusieurs États membres, permet une lecture consolidée des risques dans les zones frontalières. Ces audits transfrontaliers contribuent à produire des cartes de risques régionales et à identifier des zones de contournement réglementaire.

c. Obstacles à l'harmonisation régionale : asymétries, fragmentation juridique et vulnérabilités techniques

Malgré les efforts entrepris, plusieurs défis limitent l'effectivité de l'harmonisation LBC/FT en Afrique centrale. D'abord, l'hétérogénéité des cadres juridiques nationaux freine la convergence. Même lorsque les États adoptent des textes alignés sur les recommandations du GAFI, les définitions de concepts clés comme la propriété effective ou les seuils de déclaration peuvent varier (Godefroy et al., 2011). Cela permet aux criminels de tirer parti de l'arbitrage réglementaire en exploitant les juridictions les moins strictes. Ensuite, les disparités de capacités entre CRF sont marquées. Certaines disposent d'outils modernes, d'équipes spécialisées et d'accès à des données multidimensionnelles. D'autres peinent à traiter les STR dans des délais raisonnables, ce qui nuit à l'efficacité des enquêtes croisées (Akinteye et al., 2023). L'interopérabilité juridique pose également problème. Les accords d'entraide judiciaire existants n'harmonisent pas toujours les seuils de preuve, ni les normes de protection des données. Des divergences sur les lois de confidentialité peuvent ralentir, voire empêcher, le partage d'informations cruciales entre États (Quintel, 2022). Enfin, l'intégration technologique, bien que priorisée, reste entravée par des différences d'infrastructure, des formats de données incompatibles et des niveaux hétérogènes de cybersécurité. Certaines plateformes régionales prévues pour accélérer les alertes sont sous-utilisées, par crainte d'exposer des données sensibles.

d. Réponses stratégiques : vers une harmonisation fonctionnelle

Face à ces défis, plusieurs pistes sont envisagées pour améliorer la cohérence régionale. Cela passe d'abord par une meilleure normalisation des textes juridiques, via des lois modèles régionales transposées de manière uniforme. Ensuite, un investissement conjoint dans les technologies (KYC, biométrie, systèmes d'analyse prédictive) permettrait de niveler les capacités techniques des CRF et des banques. Des formations communes, des inspections croisées et des bibliothèques typologiques partagées permettraient d'unifier les cultures de supervision, en alliant rigueur réglementaire et approche proportionnée. L'extension de la surveillance aux secteurs non bancaires, notamment ceux fortement impliqués dans les flux de valeur (or, immobilier, transfert d'argent), reste également un chantier critique. Enfin, les pressions internationales liées aux notations du GABAC et aux attentes des correspondants bancaires pourraient être utilisées comme levier d'unification, en responsabilisant les membres performants pour soutenir ceux en retard, sous peine de pénaliser collectivement l'accès aux marchés internationaux (Ryder, n.d.).

L'architecture LBC/FT en Afrique centrale et plus largement sur le continent africain est en cours de transformation. L'adoption de standards internationaux, la montée en puissance des CRF, la coordination régionale via des organes comme le COBAC ou le GIABA, témoignent d'une dynamique d'harmonisation avancée. Toutefois, sans convergence effective des pratiques, ni renforcement des capacités des maillons faibles, cette harmonisation restera partielle et inefficace. Seule une approche fonctionnelle, intégrant technologie, coopération et responsabilisation commune, permettra de faire face aux risques systémiques et aux menaces transnationales qui pèsent sur la stabilité financière du continent.

3. Cadre législatif national et rôle de l'ANIF

a. Loi congolaise sur la LCB-FT

En République du Congo, la lutte contre le blanchiment de capitaux et le financement du terrorisme (LCB-FT) s'inscrit dans une démarche visant à intégrer les normes internationales dans le droit interne. La loi n°37-2008, initialement adoptée pour encadrer les pratiques financières illicites, a été révisée en 2020 afin d'incorporer les exigences du Groupe d'Action Financière (GAFI) et de répondre aux évaluations régionales menées par le GABAC et la COBAC. Cette modification vise à renforcer le cadre juridique face aux évolutions des menaces et à assurer la conformité avec les standards mondiaux.

La version révisée de la loi apporte trois changements principaux. Premièrement, elle prévoit l'incrimination pénale du blanchiment sous toutes ses formes, ce qui élargit les infractions sous-jacentes aux délits financiers tels que la corruption, le trafic de ressources naturelles et le financement de groupes armés. Selon Unger & Ferwerda (2011), *« l'élargissement du spectre des infractions sous-jacentes est une condition nécessaire pour éviter les failles juridiques dans lesquelles les criminels exploitent les zones grises »*.

Deuxièmement, la loi impose aux banques et institutions financières l'obligation de déclarer toute opération suspecte dans un délai de 48 heures auprès de l'Agence Nationale d'Investigation Financière (ANIF). Cette mesure s'inscrit dans le contexte du suspicious activity reporting. Levi & Reuter (2006) indiquent que *« l'efficacité du système mondial de LCB-FT repose largement sur la qualité, la rapidité et l'exhaustivité des déclarations transmises par les acteurs financiers de première ligne »*. Le Congo a ainsi introduit une obligation de rapidité pour améliorer le dispositif national de détection.

Troisièmement, la loi exige la conservation des données financières et de vigilance pendant au moins 10 ans. Cette disposition répond aux besoins de traçabilité des flux financiers et permet aux autorités judiciaires et de supervision d'accéder à un historique suffisant pour enquêter sur des schémas complexes ou différés de blanchiment. Dans la littérature, Sharman (2011) affirme que *« sans conservation prolongée des données, la détection et la preuve judiciaire du blanchiment deviennent quasi impossibles dans un système mondialisé »*.

La loi renforce également le rôle de l'ANIF, qui devient l'entité centrale de collecte, d'analyse et de diffusion des informations liées aux opérations suspectes. Sur le modèle des Financial Intelligence Units (FIU) promues par le GAFI, l'ANIF congolaise centralise les déclarations de soupçons, mène des investigations préliminaires et transmet les dossiers pertinents aux autorités judiciaires. Nkouka (2020) note que *« l'ANIF est l'articulation entre la vigilance bancaire et la répression judiciaire, transformant l'information brute en renseignement exploitable »*.

La réforme législative de 2020 cherche aussi à adapter les normes internationales aux *réalités locales. La prévalence de l'économie informelle et des transactions en espèces au Congo accroît certains risques. La loi met donc l'accent sur la vigilance dans les s*ecteurs non bancarisés, chez les professions non financières désignées (avocats, notaires, agents immobiliers) et concernant les flux transfrontaliers. Barth, Caprio & Levine (2013) précisent que « la robustesse du système LCB-FT ne se limite pas au secteur bancaire, mais doit englober l'ensemble des acteurs exposés aux risques de détournement des circuits financiers ».

Cependant, malgré le renforcement du cadre légal, des défis demeurent dans sa mise en œuvre. La littérature signale des limitations en matière de capacités institutionnelles, des ressources techniques limitées pour l'ANIF et une lenteur dans la coopération interinstitutionnelle. Rose-Ackerman & Palifka (2016) observent que *« dans les pays où la gouvernance reste fragile, l'efficacité des dispositifs LCB-FT dépend autant de la volonté politique que de la qualité des textes juridiques »*.

En conclusion, la loi congolaise n°37-2008, révisée en 2020, marque une étape importante dans l'adaptation du Congo aux normes internationales de LCB-FT. Elle illustre un processus d'alignement sur les standards mondiaux tout en prenant en compte les vulnérabilités propres au contexte local. Pour les établissements bancaires comme BGFIBANK Congo, ce cadre législatif requiert une vigilance accrue et représente également un gage de crédibilité internationale, essentiel pour maintenir des relations bancaires correspondantes et garantir un accès au système financier international.

b. L'Agence Nationale d'Investigation Financière (ANIF)

Créée en 2007, l'Agence Nationale d'Investigation Financière (ANIF) du Congo constitue l'unité de renseignement financier (URF) nationale, alignée sur le modèle promu par le GAFI. Sa mission principale est de centraliser et d'exploiter les déclarations d'opérations douteuses (DOD) transmises par les banques et autres entités assujetties, de coopérer avec les autorités judiciaires nationales et internationales, et de produire des analyses stratégiques permettant de mieux comprendre les tendances du blanchiment de capitaux et du financement du terrorisme (BC/FT). Comme le rappellent Unger & Ferwerda (2011), *« l'efficacité d'une URF dépend de sa capacité à transformer des données brutes en renseignement financier exploitable »*.

Le rôle de l'ANIF est donc double : opérationnel et stratégique. Sur le plan opérationnel, elle reçoit, analyse et filtre les DOD afin d'identifier les transactions suspectes qui méritent une transmission aux parquets compétents. Cette fonction est essentielle, car elle évite aux autorités judiciaires d'être submergées par un flux massif de données, en leur fournissant des dossiers structurés. Sur le plan stratégique, l'ANIF publie des rapports annuels qui visent à identifier les tendances émergentes et à orienter les politiques publiques. Selon Nkouka (2020), *« l'ANIF joue un rôle de vigie macro-financière, en éclairant les décideurs sur les zones de vulnérabilité du système »*.

Les statistiques récentes confirment l'importance croissante de cet organe. D'après le rapport ANIF 2023, le nombre de DOD issues du secteur bancaire a progressé de 35 % en une année, ce qui illustre à la fois une meilleure sensibilisation des acteurs bancaires et une pression réglementaire accrue exercée par la COBAC et le GABAC. Cette évolution est cohérente avec les constats de Reuter & Truman (2004), selon lesquels *« la montée en puissance des unités de renseignement financier se traduit généralement par une augmentation rapide et soutenue des déclarations de soupçons, reflet de la maturation des dispositifs nationaux »*.

En outre, l'ANIF développe une coopération active avec les instances internationales telles que le GABAC, le GAFI ou le Groupe Egmont, réseau mondial des unités de renseignement financier. Cette coopération facilite les échanges transfrontaliers d'informations, indispensables dans une région marquée par des flux illicites transnationaux (trafic de ressources naturelles, contrebande, financement de groupes armés). Comme le soulignent Ferwerda & Reuter (2019), *« la criminalité financière ignore les frontières, et seule une coopération internationale robuste permet de réduire l'asymétrie d'information entre les juridictions »*.

Toutefois, malgré ses avancées, l'ANIF fait face à des défis structurels. Le premier est lié à la limitation de ses ressources techniques et humaines, qui restreint sa capacité d'analyse approfondie. Le second réside dans la lenteur des suites judiciaires, qui peut décourager les déclarants si leurs signalements n'aboutissent pas à des sanctions visibles. Enfin, la fragilité institutionnelle du pays accroît le risque d'ingérence politique, comme l'ont souligné Rose-Ackerman & Palifka (2016), pour qui *« la durabilité des institutions de lutte contre le blanchiment repose sur leur indépendance effective et leur protection contre la capture politique »*.

En définitive, l'ANIF Congo représente une pièce maîtresse du dispositif national de LCB-FT. Son action, encore perfectible, a néanmoins contribué à renforcer la culture de conformité dans le secteur bancaire, à améliorer la coopération internationale et à doter le Congo d'une structure de vigilance systémique. Pour les établissements comme BGFIBANK Congo, la montée en puissance de l'ANIF se traduit par une exigence accrue en matière de reporting et de diligence, mais elle constitue également une garantie de crédibilité face aux partenaires internationaux.

L'examen du cadre normatif et institutionnel de la lutte contre le blanchiment de capitaux et le financement du terrorisme (LCB-FT) met en évidence l'articulation entre normes internationales, régulations régionales et dispositifs nationaux. À l'échelle globale, le GAFI, à travers ses 40 Recommandations et son mécanisme d'évaluation mutuelle, constitue le socle des standards appliqués par les États et les institutions financières. L'ONUDC, par ses conventions juridiquement contraignantes, a renforcé ce dispositif en érigeant le blanchiment et la corruption en infractions transnationales, appelant à une coopération judiciaire accrue. Le Comité de Bâle, quant à lui, a intégré

les risques de criminalité financière dans le champ de la régulation prudentielle, faisant de la conformité un enjeu stratégique de gouvernance bancaire.

Dans l'espace CEMAC, le GABAC et la COBAC traduisent ces exigences internationales en règles contraignantes, cherchant à harmoniser les pratiques tout en tenant compte des vulnérabilités locales. Enfin, au niveau national, la loi congolaise révisée et l'action de l'ANIF illustrent l'effort d'adaptation aux standards mondiaux, malgré des contraintes structurelles persistantes.

Cette construction normative et institutionnelle constitue une base indispensable, mais elle ne peut suffire sans outils de détection performants et sans innovations technologiques capables d'anticiper et de contrer l'évolution des menaces. C'est précisément l'objet du chapitre 3, consacré aux dispositifs de détection et aux solutions technologiques émergentes.

Chapitre 3 – Dispositifs de détection des transactions suspectes : panorama, limites et comparatifs internationaux

Si l'architecture normative internationale fournit un cadre indispensable à la lutte contre le blanchiment de capitaux et le financement du terrorisme (LCB-FT), son efficacité dépend largement de la capacité opérationnelle des institutions financières à détecter les comportements à risque en temps réel. C'est à ce carrefour entre exigence réglementaire et réponse technique que se situent les dispositifs de détection des transactions suspectes.

Dans un contexte où les criminels financiers s'appuient sur des schémas de plus en plus sophistiqués — tels que le fractionnement des opérations, l'utilisation de sociétés-écrans ou le financement par micro-transferts — les méthodes traditionnelles de surveillance apparaissent progressivement obsolètes ou structurellement insuffisantes (*FATF, 2022* ; *World Bank, 2021*). De surcroît, les spécificités économiques et institutionnelles de certaines régions, notamment en Afrique centrale, ajoutent des couches de complexité supplémentaires : informalité dominante, accès limité aux données numériques, et faible capacité analytique des cellules conformité.

Ce chapitre s'attache à explorer les mécanismes en place dans les établissements bancaires, tant dans l'espace CEMAC qu'à l'échelle internationale. Il distingue les approches traditionnelles (reposant sur des seuils et règles fixes), des dispositifs plus structurés fondés sur le comportement ou les typologies de risque. Il met également en lumière le rôle central des organes de contrôle, tels que l'ANIF ou la COBAC, dans la régulation des systèmes de surveillance interne.

Au-delà des pratiques locales, une analyse comparative des systèmes internationaux (États-Unis, Union Européenne, pays africains hors CEMAC) permet de situer les performances et lacunes du modèle congolais, et d'identifier des leviers d'optimisation pour les chapitres à venir. L'objectif est ici d'établir une cartographie critique des dispositifs actuels, qui servira de socle au diagnostic spécifique de BGFIBANK Congo dans la Partie II, et aux recommandations technologiques, organisationnelles et humaines qui structureront la Partie III.

1. Les différentes typologies du blanchiment de capitaux et du financement du terrorisme

a. Le blanchiment de capitaux

Modèle en trois étapes : placement, superposition et intégration

Le modèle en trois étapes du placement, de la superposition et de l'intégration demeure fondamental pour comprendre comment les fonds illicites circulent avant d'être absorbés dans l'économie légitime. Chacune de ces phases présente des caractéristiques propres et des vulnérabilités spécifiques, influençant directement la conception des dispositifs de détection dans les institutions financières.

La phase de **placement** consiste à introduire les produits illicites dans le système financier. Elle se fait fréquemment par dépôts d'espèces, parfois structurés pour éviter les seuils de déclaration. Dans des économies à forte intensité de cash, comme la République du Congo, où le faible taux de bancarisation favorise l'usage massif de liquidités, les criminels dissimulent leurs fonds via des encaissements commerciaux ordinaires (Utkina et al., 2023). Les commerces de détail, bars ou stations-service servent souvent de façades, leurs revenus étant artificiellement gonflés pour justifier des dépôts réguliers.

D'autres vecteurs incluent l'achat d'instruments monétaires (chèques de banque, mandats) ou l'usage de produits de passerelle (cartes prépayées). Pour des banques comme BGFIBANK Congo, la vigilance doit porter sur les comptes nouvellement ouverts présentant des comportements de dépôts incohérents avec l'activité déclarée (Palakurti, 2023).

La **superposition** ajoute une complexité destinée à obscurcir la piste d'audit. Les criminels multiplient les transferts entre comptes, juridictions et classes d'actifs afin de générer une opacité transactionnelle (Bakry et al., 2024). Ces mouvements vont du simple virement intrabancaire à des transferts transfrontaliers utilisant plusieurs intermédiaires, exploitant les délais procéduraux et les régimes de confidentialité bancaire. Les opérations de change répétées sans justification économique constituent une technique fréquente, brouillant le suivi de la valeur (Helgesson & Mörth, 2018). Le commerce sert également de canal : surfacturation ou sous-facturation masquent des transferts de valeur sous couverture légale (Godefroy et al., 2011). La superposition peut aussi prendre la forme de transferts circulaires entre entités liées, ponctués de paiements vers des tiers non reliés, avant de revenir au contrôle des bénéficiaires effectifs. Les outils traditionnels de surveillance peinent à détecter ces schémas. D'où la nécessité d'approches d'anomalie transactionnelle et d'analyses multi-nœuds, comme l'analyse de réseaux sociaux (SNA), qui révèlent des grappes suspectes incompatibles avec des comportements commerciaux légitimes (Shaikh et al., 2021).

L'**intégration** marque la réintroduction des fonds blanchis dans l'économie légale, sous forme de revenus ou d'investissements apparemment conformes. Les actifs visés incluent l'immobilier, les véhicules de luxe ou encore des entreprises-écrans créées pour générer des flux « propres » (Utkina et al., 2023). À ce stade, les profils financiers ressemblent à ceux d'acteurs honnêtes, compliquant la détection. Les indicateurs résident dans des incohérences entre la capacité économique observable d'une entité et l'ampleur de ses investissements (Godefroy et al., 2011). Lorsque des capitaux illicites servent de garanties financières, ils peuvent se fondre derrière une documentation conforme, sauf si une diligence renforcée révèle des anomalies. Les défaillances dans les registres de bénéficiaires effectifs accentuent la difficulté. Les environnements permissifs en matière d'investissement constituent ainsi des terrains propices à l'intégration (Quintel, 2022).

Les défis sont amplifiés dans des contextes transfrontaliers. Durant le placement, certains pays appliquent un KYC insuffisant, permettant des dépôts suspects. La superposition tire profit de la fragmentation entre juridictions, et l'intégration exploite les failles dans la transparence des bénéficiaires effectifs. Ces réalités justifient le renforcement de la coopération interinstitutionnelle et du partage d'informations en temps réel. Les cellules de renseignement financier et les réseaux comme le Groupe Egmont permettent de transférer des signaux suspects d'un acteur à un autre, améliorant la détection globale (Helgesson & Mörth, 2018).
Les systèmes de mobile money brouillent encore davantage les frontières entre les étapes. Des fonds peuvent être placés via des dépôts fractionnés par des agents locaux (placement), agrégés sur des comptes liés (superposition), puis rapidement dirigés vers l'achat d'actifs (intégration) (YANG, 2018). La vitesse de circulation sur les plateformes numériques dépasse largement celle des rails bancaires classiques, ce qui oblige les institutions à revoir leurs algorithmes de détection. Plutôt que de s'appuyer sur une séquence stricte entre étapes, les modèles doivent reconnaître la simultanéité et la convergence de plusieurs typologies dans des délais raccourcis.
Dans l'environnement opérationnel de BGFIBANK Congo, ces vulnérabilités se matérialisent de manière concrète : opportunités de placement liées à la contrebande le long des frontières instables (Godefroy et al., 2011), risques de superposition via les corridors commerciaux et leurs pratiques de facturation douteuses (Helgesson & Mörth, 2018), et intégration facilitée par l'absence de registres complets de propriété effective (Akinteye et al., 2023). La riposte nécessite trois axes : vigilance renforcée dans les secteurs manipulant d'importants volumes de cash, intégration d'analyses avancées pour suivre les flux non linéaires, et due diligence élargie pour relier les transactions aux historiques d'acquisition d'actifs.

En somme, bien que le modèle soit présenté en étapes distinctes, le placement, la superposition et l'intégration forment un continuum. La perturbation d'une seule phase peut entraver l'ensemble du processus de blanchiment. La stratégie la plus efficace repose sur des contrôles ciblés, adaptés aux risques locaux mais éclairés par l'intelligence typologique mondiale. Ce n'est qu'en combinant vigilance contextuelle, outils technologiques avancés et coopération internationale que les institutions financières pourront contrer efficacement les stratégies sophistiquées de BA/FT.

Le blanchiment basé sur le commerce (TBML)

Le blanchiment d'argent basé sur le commerce (TBML) est l'une des typologies les plus sophistiquées, exploitant la complexité et le volume élevé des transactions internationales pour masquer les transferts de valeur illicites. Il détourne les cadres commerciaux légitimes par la manipulation des documents, des prix et des descriptions de marchandises, permettant ainsi de dissimuler des produits criminels ou des financements terroristes derrière une activité d'import-export apparemment régulière. Les pratiques courantes incluent la surfacturation, la sous-facturation, la falsification des quantités, la facturation multiple ou l'étiquetage inexact des produits (Godefroy et al., 2011).
Le principal défi pour les institutions financières est de distinguer les écarts commerciaux légitimes, dus aux fluctuations des prix ou à la qualité des biens, des manipulations délibérées. Les criminels ciblent souvent des secteurs où les prix sont volatils, comme les matières premières. En République du Congo, où les exportations de ressources minières dominent, cette volatilité sert de couverture aux écarts de facturation (Helgesson & Mörth, 2018). Répétés sur plusieurs expéditions, ces écarts transfèrent d'importantes valeurs en évitant la détection des systèmes classiques de surveillance des transactions.
La complexité est renforcée par l'usage d'intermédiaires et de routes maritimes indirectes, notamment par des ports ou zones de libre-échange à faible contrôle. Ainsi, la détection efficace du TBML exige une corrélation multidimensionnelle des données au-delà des seuils monétaires. Les algorithmes d'apprentissage automatique se révèlent particulièrement adaptés : régression logistique, forêts aléatoires et réseaux neuronaux évaluent les ratios prix/poids, la fréquence des expéditions, les profils de contrepartie et les risques pays pour prédire la probabilité de TBML (Ji, 2023). Les méthodes non supervisées, comme le clustering, identifient les valeurs aberrantes, par exemple des expéditions à prix constamment supérieurs à ceux des pairs malgré une origine et une qualité similaire.
La surveillance nécessite également l'intégration de données massives : factures, connaissements, avis de paiement, mais aussi rapports d'inspection ou informations ouvertes défavorables sur les contreparties.
Le TBML exploite aussi les asymétries régionales. Dans la zone CEMAC, la coopération douanière limitée facilite les détournements : des expéditions transitent par des États aux contrôles plus faibles avant d'être réintégrées dans le circuit financier (Godefroy et al., 2011). La coopération interinstitutionnelle et le partage transfrontalier via le Groupe Egmont réduisent ces vulnérabilités en accélérant la circulation des signaux d'alerte (Quintel, 2022).
Il existe également un chevauchement entre TBML et financement du terrorisme. Si le blanchiment vise à légitimer des fonds criminels, le financement terroriste détourne parfois les mécanismes commerciaux pour approvisionner des zones de conflit. Ainsi, des envois surfacturés de biens humanitaires peuvent masquer un soutien logistique à des groupes armés (Ryder, n.d.). Les algorithmes doivent donc combiner des critères de tarification anormaux avec des indicateurs géographiques liés aux zones sanctionnées.
Sur le plan technologique, les systèmes de gestion des règles d'affaires (BRMS) combinés à l'IA offrent un avantage stratégique. Ils automatisent la mise à jour des typologies TBML publiées par les CRF ou le GAFI, maintenant la conformité en temps réel (Palakurti, 2023). En parallèle, l'analyse des réseaux sociaux (SNA) cartographie les relations complexes entre exportateurs, importateurs, transitaires, courtiers et banques. Cette approche permet d'identifier les nœuds centraux des réseaux de blanchiment, dont la neutralisation perturbe l'ensemble du dispositif criminel (Shaikh et al., 2021).

En conclusion, la lutte contre le TBML requiert une combinaison d'expertise commerciale (connaissance des flux sectoriels et des prix), de capacités analytiques avancées (IA, big

data, SNA), et de coopération multi-juridictionnelle. Pour les institutions congolaises dépendantes des flux de matières premières, comme BGFIBANK Congo, seule une gouvernance robuste et une adaptation continue des contrôles permettront de contrer cette typologie parmi les plus difficiles du blanchiment d'argent.

Les Sociétés écrans et structures complexes

Le recours à des sociétés écrans et à des structures d'entreprise complexes constitue une méthode bien établie pour dissimuler la propriété effective et séparer les fonds illicites de leurs origines criminelles, compliquant leur détection par les autorités et les institutions financières. Ces entités, souvent créées dans des juridictions où les règles de transparence sont faibles et la confidentialité juridique élevée, offrent un vernis de légitimité exploitable par des montages multi-niveaux impliquant fiducies, prête-noms et participations croisées (Godefroy et coll., 2011). Elles permettent ainsi de disperser la valeur entre plusieurs véhicules juridiques tout en conservant un contrôle indirect par des bénéficiaires non divulgués.

Dans les canaux bancaires, de telles entités peuvent apparaître comme des clients ordinaires, dotés de statuts conformes, mais dépourvus d'activité commerciale réelle. Sans protocoles robustes de vérification de la propriété effective alignés sur les recommandations du GAFI (Utkina et al., 2023), ces structures passent la due diligence initiale. Le risque est accru dans les juridictions où l'enregistrement peut être délégué à des cabinets d'avocats ou agents spécialisés, qui masquent les véritables bénéficiaires. La complexité croît lorsque ces coquilles sont articulées en chaînes multi-juridictionnelles : une société congolaise peut appartenir à une holding offshore, elle-même contrôlée par un trust étranger, chaque lien bloquant l'enquête en l'absence de coopération internationale (Quintel, 2022).

Les secteurs extractifs, exposés à des flux transfrontaliers complexes, sont particulièrement vulnérables. Les criminels reproduisent des structures utilisées légitimement dans les coentreprises pour investir des fonds blanchis dans des concessions minières. La distinction repose alors sur une diligence renforcée incluant la vérification de la chaîne d'approvisionnement et le filtrage médiatique défavorable (Akinteye et al., 2023). Dans le commerce international, des coquilles de façade des deux côtés des flux facilitent la facturation fictive ou les expéditions fantômes : une entité écran émet des factures gonflées et son homologue paie via un réseau bancaire, paraissant conforme (Helgesson & Mörth, 2018). Ces structures recourent aussi à des prêts interentreprises ou à des accords de services fictifs. Des paiements qualifiés de « frais de gestion » ou « redevances » peuvent transférer des montants importants à l'étranger avec peu de preuves tangibles.

Dans le financement du terrorisme, des architectures similaires servent à rediriger des dons caritatifs légitimes vers des entités affiliées à des réseaux extrémistes (Ryder, s.d.). La détection requiert alors une cartographie relationnelle grâce à l'analyse des réseaux sociaux (SNA), révélant des liens cachés entre administrateurs, actionnaires et contreparties (Shaikh et al., 2021).

Les risques varient selon les juridictions. Certaines offrent des services d'incorporation de masse produisant des coquilles « prêtes à l'emploi » avec comptes bancaires déjà établis, ce qui permet d'éviter les contrôles initiaux (Godefroy et al., 2011). L'absence d'obligation de mise à jour des registres de propriété accentue l'opacité : le contrôle peut changer de mains plusieurs fois sans divulgation. Pour une banque comme BGFIBANK Congo, se fier uniquement aux documents fournis par le client revient à intégrer des structures opaques. Les contre-mesures exigent des vérifications multi-sources, en croisant les registres nationaux et bases de données commerciales mondiales (Akinteye et al., 2023). En l'absence de registres fiables, des attestations notariées indépendantes peuvent être exigées, bien que leur authenticité doive être vérifiée (Helgesson & Mörth, 2018).

La reconnaissance de motifs récurrents constitue un autre levier : des clients partageant des adresses, utilisant les mêmes agents de création de sociétés ou effectuant des transactions séquentielles avec factures chevauchantes. Ces indices isolés prennent sens collectivement. L'intelligence artificielle appliquée aux graphes de relations permet d'identifier des nœuds de contrôle cachés, reliant plusieurs coquilles dans divers secteurs et zones (Palakurti, 2023). Ces modèles combinent données transactionnelles, registres publics, dossiers douaniers, litiges et informations médiatiques pour prioriser

les enquêtes. Les entreprises à faible risque initial peuvent être reclassées si leurs administrateurs apparaissent liés à des réseaux opaques, conformément aux attentes du Comité de Bâle sur la CDD continue (Utkina et al., 2023).

Les réformes visant à accroître la transparence, telles que les registres centralisés de bénéficiaires effectifs, constituent un progrès, mais leur mise en œuvre reste inégale (Godefroy et al., 2011). En République du Congo, malgré des initiatives récentes, les capacités de numérisation limitées retardent l'accès en temps réel aux données, ouvrant la voie à des abus si les banques s'appuient uniquement sur ces registres (Akinteye et al., 2023). Les établissements doivent donc construire des bases de données internes sur les bénéficiaires effectifs, alimentées lors de l'intégration et des mises à jour régulières, permettant d'identifier des anomalies dans le temps.

Pour les autorités, le retraçage des fonds via des sociétés écrans exige des mécanismes de coopération juridique bilatéraux ou multilatéraux pour garantir la recevabilité des preuves (Quintel, 2022). Dans des forums comme la CEMAC, l'échange de typologies sur les structures opaques améliore la détection préventive et réduit la propagation de schémas criminels entre pays voisins (Helgesson & Mörth, 2018).

En définitive, la menace ne réside pas dans l'existence des sociétés écrans, parfois utiles commercialement, mais dans leur exploitation pour masquer des activités illicites. Les contre-mesures reposent sur l'harmonisation des normes de transparence, l'intégration de capacités analytiques avancées et l'automatisation. Pour des banques exposées comme BGFIBANK Congo, combiner expertise humaine, outils technologiques et coopération internationale est indispensable pour réduire la vulnérabilité face à des criminels exploitant la complexité juridique pour blanchir des fonds ou financer le terrorisme.

b. Le financement de terrorisme

Utilisation abusive des organismes de bienfaisance et à but non lucratif

Les organismes de bienfaisance et à but non lucratif remplissent des fonctions humanitaires, religieuses, éducatives et sociales essentielles, mais présentent aussi des vulnérabilités exploitables pour le financement du terrorisme (FT). Leur capacité à collecter et distribuer des sommes importantes avec une perception positive du public, une autonomie relative et parfois une surveillance réduite accroît leur profil de risque. Celui-ci découle de sources de financement variées, de transferts transfrontaliers fréquents vers des zones à haut risque, du recours à des intermédiaires difficiles à contrôler et d'exemptions réglementaires historiquement justifiées pour encourager l'engagement civique. Ces caractéristiques peuvent être détournées par l'infiltration de réseaux extrémistes, l'exploitation de lacunes de gouvernance ou la création d'organisations fictives destinées à canaliser des ressources vers des entités interdites (Ryder, n.d.).

Un scénario courant consiste à détourner les dons sous prétexte de secours humanitaires. Une organisation peut collecter des fonds pour des victimes d'un conflit, tout en confiant la mise en œuvre à des partenaires liés à des groupes extrémistes. Les décaissements, bien que partiellement utilisés pour l'aide, servent aussi à financer des opérations ou à rémunérer des fournisseurs sympathisants (Godefroy et al., 2011). Ces activités hybrides compliquent la détection, car elles s'accompagnent souvent de livraisons documentées. Dans d'autres cas, des entités caritatives fictives n'existent que comme façades : elles collectent des fonds, notamment via les diasporas et des systèmes de transfert, avant de les envoyer à des bénéficiaires affiliés à l'étranger (Helgesson & Mörth, 2018). L'absence de dépenses locales vérifiables, comme des salaires ou des registres de distribution, constitue un signal d'alerte.

Des techniques de superposition semblables à celles du blanchiment sont également utilisées : les fonds transitent par plusieurs ONG intermédiaires dans différentes juridictions avant d'être intégrés à des projets contrôlés par des bénéficiaires liés. Les faiblesses des régimes d'enregistrement, notamment le manque de transparence sur la propriété effective, aggravent le problème (Utkina et al., 2023). Certaines organisations exploitent aussi des entreprises sociales affiliées, générant des revenus de ventes gonflés

artificiellement par des transactions avec des sympathisants, blanchissant ainsi des fonds sous couvert d'activité économique caritative.

Les flux géographiques sont un indicateur clé : des transferts répétés vers des juridictions inscrites sur les listes à haut risque du GAFI ou vers des zones en conflit justifient une vigilance accrue (Ryder, n.d.). Les institutions financières doivent donc adapter leur suivi : non seulement surveiller les seuils de valeur, mais aussi détecter des changements comportementaux comme une expansion soudaine dans des zones à haut risque ou des volumes de transactions anormaux par rapport aux cycles habituels (Palakurti, 2023). Les contreparties doivent être contrôlées via les listes de sanctions et bases de données défavorables, et les profils clients mis à jour à partir des informations transmises par les CRF (Helgesson & Mörth, 2018).

Les rapports d'opérations suspectes liés aux abus caritatifs doivent inclure des preuves documentaires d'anomalies : factures incohérentes, absence d'autorisations d'expédition, ou demandes de subventions identiques envoyées à différents bailleurs. L'analyse relationnelle de ces données permet de relier des cas distincts à travers des signataires, fournisseurs ou fiduciaires communs, renforcée par l'analyse des réseaux sociaux (SNA), qui met en lumière les acteurs centraux (Shaikh et al., 2021).

La réglementation évolue pour mieux encadrer le secteur. Le GAFI, via sa recommandation 8, insiste sur la nécessité de protéger les ONG contre l'exploitation terroriste sans restreindre leur action (Ryder, n.d.). Les bonnes pratiques incluent la séparation des responsabilités au sein des conseils d'administration, des audits indépendants, la tenue de registres détaillés des bénéficiaires et la divulgation rapide des transferts transfrontaliers (Akinteye et al., 2023). Dans des environnements à ressources limitées comme la République du Congo, la sensibilisation sectorielle menée par les régulateurs et les CRF demeure cruciale.

La prévention et la détection de l'abus des organismes caritatifs nécessitent des défenses combinées : renforcement de la gouvernance interne des associations, amélioration du KYC/EDD adapté au secteur, partage accru d'informations entre banques et autorités, sensibilisation réglementaire ciblée et adoption de technologies de surveillance dynamique. Ces mesures permettent de protéger les flux légitimes tout en limitant les risques que les ONG deviennent, volontairement ou non, des facilitateurs de financements terroristes.

Entreprises à forte intensité de liquidité

Les entreprises à forte intensité numéraire représentent une menace centrale en matière de blanchiment d'argent et de financement du terrorisme en raison de leur dépendance structurelle aux flux importants de monnaie physique. Bars, restaurants, établissements de jeux, stations-service, lave-autos et commerces de détail dans des environnements où les paiements électroniques restent marginaux offrent un terrain propice à l'intégration des fonds illicites. Les dépôts fréquents d'espèces s'intègrent sans difficulté dans les revenus légitimes, rendant l'intrusion de fonds criminels difficile à détecter (Utkina et al., 2023). Dans des juridictions où l'utilisation du cash domine, comme la République du Congo, la surveillance est limitée par la faible pénétration bancaire et le recours réduit aux paiements numériques. Cette dépendance rend les mécanismes de détection traditionnels inefficaces : même des dépôts élevés semblent normaux dans ces contextes si les modèles reposent sur des valeurs agrégées et non sur une analyse comportementale fine (Palakurti, 2023). Les criminels exploitent ces conditions en acquérant ou créant des commerces en espèces, soit réels, soit fictifs, qui servent de façade pour l'injection de capitaux illicites. Les stratégies incluent la manipulation des registres de ventes, l'ajustement artificiel des systèmes de point de vente, ou la structuration des dépôts sous les seuils réglementaires (Akinteye et al., 2023). Ces entreprises peuvent également être détournées à des fins de financement du terrorisme, en canalisant une partie de leurs bénéfices déclarés vers des tiers au travers de paiements fournisseurs ou de contributions « caritatives », échappant ainsi au contrôle si les vérifications de contreparties et de propriété effective restent limitées (Ryder, n.d. ; Godefroy et al., 2011). Dans les zones frontalières où la régulation est faible, elles servent souvent de points de collecte pour transférer physiquement les fonds vers des juridictions voisines. Pour les institutions financières, la vigilance doit dépasser la simple analyse des volumes pour inclure des indicateurs contextuels : incohérences entre dépôts et activité

visible (trafic, heures d'ouverture), variations géographiques inhabituelles dans l'approvisionnement des fournisseurs, ou utilisation disproportionnée des services de coffre (Helgesson & Mörth, 2018). La détection doit aussi intégrer le croisement des données fiscales avec les flux bancaires pour identifier des revenus artificiellement gonflés. Le recours aux informations fournies par les CRF permet d'affiner ces paramètres (Godefroy et al., 2011). Les technologies renforcent cette capacité : l'intelligence artificielle permet de modéliser les comportements sectoriels et d'identifier les valeurs aberrantes (Palakurti, 2023). L'analyse des réseaux sociaux (SNA) peut révéler des liens entre plusieurs entreprises distinctes servant un même réseau de blanchiment (Shaikh et al., 2021). Le risque est accru lorsque les structures de propriété sont opaques ou transitent par des sociétés de portefeuille fictives, notamment dans le cas de franchises, où la présence d'une marque donne une légitimité apparente (Akinteye et al., 2023).

Ces vulnérabilités se retrouvent aussi dans les entreprises hybrides, par exemple lorsqu'un bureau de change opère dans un commerce en espèces, introduisant des risques liés aux transactions forex (Helgesson & Mörth, 2018). Les paiements mobiles ajoutent une complexité supplémentaire : les fonds déposés en magasin peuvent être rapidement dispersés entre plusieurs portefeuilles, échappant à une surveillance consolidée (YANG, 2018). Cela exige une intégration complète des données entre banques et fintechs pour reconstituer les profils comportementaux.

La réponse inclut des mesures réglementaires et sectorielles. Le GAFI recommande des programmes de sensibilisation pour les propriétaires de ces entreprises, des obligations de tenue de registres renforcées, et parfois des exigences de déclaration sectorielle spécifiques (Ryder, n.d.). Pour les banques, cela implique d'intégrer des systèmes d'alerte précoce capables de réévaluer les profils de risque lors de changements majeurs : nouveaux propriétaires, diversification inhabituelle, ou expansion rapide dans des zones sensibles. Le partage d'informations avec les CRF doit être proactif afin d'anticiper les évolutions de typologies.

Système informel de transfert de valeur

Les systèmes informels de transfert de valeur (IVTS) regroupent des mécanismes permettant de transférer des fonds en dehors des canaux financiers réglementés. Ancrés culturellement dans des pratiques comme le hawala ou le hundi, ils reposent sur la confiance et des accords de compensation entre courtiers, ce qui rend les flux difficiles à détecter par les outils traditionnels de lutte contre le blanchiment (AML) et le financement du terrorisme (CTF) (Ryder, n.d.). Dans des contextes comme la République du Congo, où la bancarisation est faible et où l'économie informelle domine, ces systèmes répondent aux besoins de populations dépendantes des envois de fonds de la diaspora. Opérationnellement, un courtier local reçoit les fonds d'un expéditeur et un partenaire règle le montant équivalent au destinataire. Le règlement entre courtiers peut se faire par compensation de marchandises ou via des transactions commerciales, rendant le suivi transfrontalier presque invisible (Godefroy et al., 2011). Cette discrétion rend les IVTS attrayants mais vulnérables à l'usage abusif, notamment pour le financement du terrorisme. Dans les zones frontalières instables, ils facilitent le transfert des revenus issus de contrebande et de l'exploitation minière illicite vers des groupes armés. Le transport physique de liquidités s'insère dans les étapes de placement et de superposition, souvent via des cambistes non réglementés ou des manipulations commerciales (Utkina et al., 2023). Les envois de fonds fréquents et de faible valeur provenant de la diaspora échappent aussi aux systèmes d'alerte bancaires basés sur des seuils (Palakurti, 2023). Un risque croissant est l'hybridation avec les services numériques. Le mobile money, largement adopté pour sa commodité, peut devenir un quasi-IVTS lorsque les agents règlent leurs soldes par des accords informels plutôt que par des canaux agréés (YANG, 2018). Ces transactions accélèrent les flux tout en réduisant la traçabilité, à moins d'intégrer des données de géolocalisation et d'analyse comportementale pour détecter des itinéraires incompatibles avec les modèles habituels.

Les institutions financières peuvent être impliquées indirectement dans les règlements IVTS, par exemple lorsque les opérateurs déposent ou retirent des fonds via des micro-entreprises transfrontalières. Des dépôts suivis de transferts sortants sous les seuils de déclaration peuvent sembler normaux en l'absence de détection ciblée (Akinteye et al., 2023). Les contraintes réglementaires compliquent l'atténuation : une interdiction stricte pousserait les usagers légitimes dans la clandestinité, réduisant la

coopération possible avec les courtiers. Le GAFI préconise une approche fondée sur les risques, avec licences et obligations de déclaration minimales, plutôt qu'une criminalisation générale (Ryder, n.d.).

L'efficacité de cette approche dépend des capacités institutionnelles : registres des courtiers, traitement des rapports par les CRF, et diffusion de typologies aux banques pour reconnaître des empreintes transactionnelles suspectes. Les transferts récurrents entre entités sans chiffre d'affaires réel mais actives dans des corridors à haut risque constituent un indicateur typique (Helgesson & Mörth, 2018). L'analyse des réseaux sociaux peut révéler des schémas entre expéditeurs et destinataires liés à des nœuds IVTS (Shaikh et al., 2021). Les technologies offrent des solutions supplémentaires : l'IA permet d'entraîner des modèles sur des cas confirmés pour identifier des anomalies comme l'irrégularité des fréquences de transactions ou la dispersion géographique atypique. Le partage d'informations anonymisées entre CRF via le réseau Egmont renforce la précision des détections (Quintel, 2022).

Les stratégies d'atténuation doivent équilibrer sécurité et inclusion. Les campagnes de sensibilisation le long des corridors transfrontaliers peuvent inciter les opérateurs à se conformer. Des incitations comme l'accès à des infrastructures numériques en échange du respect du KYC permettent d'intégrer progressivement les acteurs informels (Akinteye et al., 2023).

Pour BGFIBANK Congo, il est essentiel d'affiner les algorithmes internes afin d'attribuer des scores de risque plus élevés aux clients dont les comportements correspondent à des modèles IVTS, et de renforcer la coopération inter-agences par la cartographie des risques frontaliers (Godefroy et al., 2011). Une telle approche améliore la capacité d'intercepter les flux financiers illicites circulant de manière invisible entre réseaux de confiance opérant en dehors de la surveillance classique.

c. Autre type : Virements télégraphiques transfrontaliers

Les virements télégraphiques transfrontaliers présentent des vulnérabilités importantes dans la lutte contre le blanchiment d'argent et le financement du terrorisme (LBC/FT), en raison de la multiplicité des acteurs, des juridictions et des régimes réglementaires impliqués. Bien qu'ils soutiennent le commerce mondial légitime, ils sont exploités par des acteurs illicites qui fragmentent les pistes d'audit et dissimulent les bénéficiaires finaux (Helgesson & Mörth, 2018). Pour des banques comme BGFIBANK Congo, les risques proviennent autant des profils clients que des relations de correspondance bancaire et des environnements juridictionnels (Godefroy et al., 2011). Le recours aux correspondants bancaires est une voie majeure d'exposition : les banques locales, sans accès direct aux systèmes de compensation, passent par de grandes banques étrangères. Toute faiblesse d'un partenaire peut créer une vulnérabilité systémique et exposer la banque à une responsabilité juridique (McConnell, 2020). Les exigences de diligence renforcée – sur la propriété effective, l'exposition aux sanctions et la gouvernance – deviennent déterminantes pour maintenir ces relations (Helgesson & Mörth, 2018).

Sur le plan opérationnel, les criminels recourent à des techniques comme le fractionnement des fonds (« schtroumpfage »), la superposition par transferts successifs ou l'usage de sociétés écrans offshore (Godefroy et al., 2011). Les risques augmentent lorsque les corridors impliquent des juridictions sous surveillance du GAFI ou présentant des lacunes réglementaires (Akinteye et al., 2023). L'intégration de notations de risque juridictionnel dans les moteurs de traitement est essentielle pour déclencher des examens renforcés. La traçabilité est affaiblie par des formats de messages SWIFT incomplets, surtout lorsque les transactions sont regroupées en lots. L'application stricte des standards modernes comme le MT202COV est nécessaire (Eijkman, 2013). Le commerce légitime complique la détection : des factures falsifiées peuvent justifier des paiements gonflés qui masquent du blanchiment commercial (Godefroy et al., 2011). Des transferts récurrents de taille moyenne, sous couvert humanitaire, peuvent aussi financer des zones de conflit (Ryder, n.d.).

Pour contrer ces risques, les banques recourent à des systèmes d'analyse avancés. Les modèles basés sur l'IA combinent règles et détection comportementale pour repérer des anomalies comme l'augmentation soudaine de la fréquence des virements ou des changements de destination vers des zones à risque (Palakurti, 2023). L'analyse des réseaux sociaux révèle aussi des schémas cachés reliant plusieurs expéditeurs à des bénéficiaires communs (Shaikh et al., 2021). Ces approches permettent de détecter des flux concentrés vers un petit nombre de comptes étrangers.

Les virements peuvent également être alimentés par des systèmes informels de transfert de valeur (IVTS), qui injectent ensuite des fonds dans les canaux bancaires. Leur détection requiert la coopération des cellules de renseignement financier (CRF) et l'échange transfrontalier d'informations (Quintel, 2022). Les recommandations du GAFI imposent une vérification des informations sur expéditeurs et bénéficiaires pour les virements supérieurs à 1 000 USD/EUR, et des mesures renforcées pour les PPE ou les juridictions opaques (Utkina et al., 2023 ; Akinteye et al., 2023).

Une approche efficace combine profilage client granulaire, évaluation en temps réel des risques juridictionnels, contrôle des relations de correspondance bancaire, intégration des données commerciales, analyse comportementale et cartographie des réseaux. L'assimilation proactive des renseignements des CRF via des plateformes comme Egmont Secure Web renforce la précision. Enfin, des audits indépendants garantissent l'efficacité des contrôles et leur adaptation aux nouvelles typologies (Helgesson & Mörth, 2018 ; Palakurti, 2023).

2. Mécanismes technologiques de détection

a. Systèmes de surveillance des transactions (TMS)

Les systèmes de surveillance des transactions (TMS) constituent le socle opérationnel de la capacité des institutions financières à détecter, analyser et signaler les opérations suspectes dans le cadre de la lutte contre le blanchiment d'argent (AML) et le financement du terrorisme (CTF). Leur efficacité dépend d'une combinaison entre sophistication technologique, alignement avec les attentes réglementaires et adaptation aux profils de risque des clients et produits (Palakurti, 2023). Dans des juridictions à haut risque comme celle où opère BGFIBANK Congo, ces systèmes doivent aller au-delà de la conformité et devenir de véritables moteurs d'intelligence capables d'intégrer les évolutions des typologies criminelles, les menaces géographiques et les comportements atypiques.

Un TMS efficace repose d'abord sur son intégration avec les systèmes bancaires centraux, permettant une couverture complète de toutes les opérations : agences, plateformes numériques, instructions de correspondants bancaires et financements du commerce. Cela permet de consolider les données clients en profils globaux, suivis en temps réel. Si les modules fondés sur des règles restent nécessaires pour respecter les seuils réglementaires (transactions en espèces, transferts transfrontaliers), leur rigidité entraîne sous-détection et excès de faux positifs (Bakry et al., 2024 ; Akinteye et al., 2023). Pour pallier ces limites, les banques intègrent des analyses avancées, notamment l'apprentissage automatique (XGBoost, SVM, forêts aléatoires), entraîné sur des ensembles de transactions étiquetées. Ces modèles exploitent des variables de vélocité des fonds, les liens relationnels ou les scores d'anomalie afin de capter des schémas subtils échappant aux approches classiques (Bakry et al., 2024). Leur efficacité exige une gouvernance robuste : validation des caractéristiques (RFECV), réglage d'hyperparamètres (Optuna) et mises à jour périodiques des modèles en fonction des nouvelles typologies. L'analyse des réseaux sociaux (SNA) enrichit encore la détection en identifiant des structures transactionnelles en couches et des comptes jouant un rôle d'intermédiaire sans justification économique (Shaikh et al., 2021). Ce type d'analyse complète la génération d'alertes en ciblant des grappes suspectes avant que des seuils classiques ne soient franchis. La réduction des faux positifs reste une priorité, notamment via l'échantillonnage stratifié et l'ingénierie de variables tenant compte de la logique commerciale (par exemple, différencier pics saisonniers légitimes et anomalies de ventes agricoles).

Une autre dimension critique réside dans le lien entre alertes générées et gestion des cas. Les analystes doivent accéder à des données enrichies (KYC, alertes passées, évaluations de risque transfrontalières, informations défavorables médiatiques ou provenant de la CRF) pour décider rapidement du dépôt d'une déclaration d'opération suspecte (Helgesson & Mörth, 2018).

La modélisation géographique est également indispensable : les transactions doivent être pondérées en fonction du risque juridictionnel, surtout si elles concernent des corridors identifiés par le GAFI comme à haut risque. Des modèles bayésiens ou de scoring pondéré combinent risque pays, risque client et anomalies comportementales pour établir la priorité des alertes (Godefroy et al., 2011). La modélisation

sectorielle, notamment dans le financement du commerce et les changes, affine encore la détection en recoupant les factures avec des indices de marché ou en identifiant des transactions circulaires sans justification économique. Face aux contraintes de ressources, notamment en Afrique, les TMS évoluent vers des architectures hybrides combinant surveillance en temps réel pour les alertes critiques et traitement différé pour les segments à faible criticité (Akinteye et al., 2023). Ces choix équilibrent réactivité et efficacité opérationnelle. Pour maintenir la confiance des régulateurs et des correspondants, les banques doivent documenter rigoureusement l'évaluation continue de leur TMS (précision, rappel, recalibrages, tests sur cas historiques, mises à jour typologiques) conformément aux directives du Comité de Bâle (Utkina et al., 2023). Des audits internes indépendants complètent cette exigence (Akinteye et al., 2023).

Enfin, la convergence entre TMS internes et sources externes, comme les alertes FIU transmises via le Groupe Egmont ou la coopération régionale CEMAC, accroît la rapidité et la pertinence de la détection (Quintel, 2022 ; Helgesson & Mörth, 2018). Ces mécanismes, intégrés dans les systèmes de gestion des règles métier, permettent aux institutions de répondre simultanément aux menaces émergentes, transformant les TMS en outils proactifs capables de freiner significativement le blanchiment et le financement du terrorisme.

b. Applications de l'IA et du Machine Learning

L'intelligence artificielle (IA) et l'apprentissage automatique (ML) transforment la détection des transactions suspectes en allant au-delà des seuils statiques et des typologies pré-codées. Contrairement aux systèmes fondés uniquement sur des règles fixes, les modèles IA/ML apprennent à partir de données historiques couvrant activités suspectes et légitimes, produisant une notation des risques reflétant les corrélations latentes entre transactions, clients et réseaux (Paul et al., 2023). Les algorithmes mobilisés vont des classificateurs supervisés (régression logistique, forêts aléatoires, gradient boosting) aux méthodes non supervisées de clustering, capables d'ingérer des ensembles de données de haute dimension issus de multiples canaux bancaires (Shaikh et al., 2021).

Les approches supervisées sont particulièrement efficaces lorsque des données étiquetées sont disponibles. En s'appuyant sur les rapports d'opérations suspectes (STR) et sur des exemples confirmés de faux positifs, elles identifient des combinaisons multivariées révélant des flux illicites. Par exemple, des arbres de décision pondèrent l'interaction entre des hausses soudaines de volumes, des risques juridictionnels et des écarts aux normes sectorielles pour générer des scores de suspicion en temps quasi réel (Palakurti, 2023). Les institutions comme BGFIBANK Congo intègrent ces modèles dans leurs systèmes de gestion des règles métiers (BRMS), permettant une propagation instantanée des mises à jour. Les techniques non supervisées apportent une valeur complémentaire en détectant des comportements anormaux sans étiquetage préalable. Le clustering (DBSCAN) regroupe les entités en cohortes « normales » et signale les valeurs aberrantes divergentes, révélant des schémas inédits comme la superposition entre PME ou de nouveaux profils de transferts (Yu et al., n.d.). Ces anomalies alimentent ensuite les enquêtes avant le dépôt de déclarations d'opérations douteuses. L'analyse comportementale pilotée par le ML définit en outre des bases de référence individualisées par client. Les modèles séquentiels identifient des schémas de dépôts suivis de virements transfrontaliers suspects, invisibles dans des agrégats mensuels (Paul et al., 2023). Les réseaux neuronaux récurrents ou convolutifs temporels apprennent ces séquences sur de longs horizons pour améliorer la prédiction.

Les méthodes d'IA basées sur des graphes exploitent l'analyse des réseaux sociaux pour révéler des intermédiaires pivot jouant un rôle dans la dispersion des fonds (Shaikh et al., 2021). Ces informations, combinées aux scores de risque, orientent les ressources vers les acteurs stratégiques plutôt que vers les seules transactions volumineuses. Toutefois, le déploiement opérationnel exige une explicabilité suffisante pour satisfaire les régulateurs. Des outils comme SHAP (SHapley Additive exPlanations) précisent la contribution de chaque variable à un score, permettant aux analystes de justifier les décisions (Akinteye et al., 2023). Des tests a posteriori sur des cas de typologies connues garantissent une sensibilité constante malgré l'évolution criminelle (Ryder, s.d.). L'intégration des modèles doit respecter les cadres de gouvernance des données, notamment la confidentialité des identifiants lors du partage interinstitutionnel via des plateformes sécurisées comme celles inspirées du réseau Egmont (Quintel,

2022). La mise en place d'un contrôle de version assure la traçabilité des sorties d'alerte, utile en cas de litiges (Helgesson & Mörth, 2018). Les architectures hybrides, combinant règles déterministes pour les obligations réglementaires et scores probabilistes pour la hiérarchisation, offrent une efficacité accrue (Palakurti, 2023). Des boucles de rétroaction entre enquêteurs et modèles améliorent progressivement la précision tout en réduisant les faux positifs (Bakry et al., 2024).

Dans un contexte comme celui de BGFIBANK Congo, marqué par l'usage intensif du cash et la montée des transferts numériques, cette adaptabilité est essentielle pour détecter les structurations dispersées via agents mobiles et comptes classiques (Yang, 2018). Les modèles incrémentiels, réentraînés en continu avec de nouveaux exemples, réduisent le décalage entre émergence et détection des typologies, comme observé pendant la crise COVID-19 (Ryder, n.d.).

Ainsi, l'IA/ML transforme la surveillance des transactions, passant d'une détection réactive fondée sur des règles à une anticipation proactive des risques dans des environnements complexes. Avec des garde-fous en matière d'explicabilité, de gouvernance des données et de validation rigoureuse, ces approches permettent aux banques de répondre aux standards mondiaux tout en restant agiles face à des adversaires adaptatifs (Palakurti, 2023 ; Yu et al., n.d.).

c. Analyse des données et reconnaissance de formes

L'analyse des données et la reconnaissance des formes renforcent les systèmes de surveillance des transactions en permettant d'aller au-delà des règles déterministes. Ces approches facilitent l'identification adaptative des typologies connues et l'émergence de nouvelles tactiques de blanchiment et de financement du terrorisme. Les architectures modernes intègrent des données issues de plateformes centrales, bureaux de change, services mobiles et partenaires tiers dans des environnements analytiques unifiés, où informations structurées et non structurées peuvent être exploitées simultanément (Ji, 2023). Cette consolidation saisit l'empreinte comportementale complète des clients qui dispersent leurs activités pour échapper à la détection.Le pipeline analytique débute par un prétraitement rigoureux pour pallier les problèmes de qualité des données fréquents dans les marchés émergents : identifiants incomplets, codages incohérents, horodatages mal alignés. La standardisation garantit la cohérence des champs nécessaires à l'application des modèles de risque et préserve la traçabilité des données utilisées dans la génération d'alertes (Akinteye et al., 2023).

Les méthodologies de reconnaissance des formes s'appuient sur des algorithmes supervisés, lorsque des exemples étiquetés sont disponibles, tels que les machines de gradient boosting ou les architectures hybrides CNN-LSTM appliquées aux séries chronologiques. Ces modèles détectent des interactions complexes, comme des crédits répétitifs de faible valeur suivis de transferts consolidés, ou encore des variations géographiques anormales des bénéficiaires (Yu et al., n.d.). Les méthodes non supervisées, telles que k-means ou DBSCAN, identifient des valeurs aberrantes non prédéfinies, utiles pour repérer des comportements atypiques liés à des voies de transfert inhabituelles. Couplées à l'analyse géospatiale, elles révèlent des concentrations suspectes de transactions provenant ou allant vers des corridors à haut risque (Godefroy et al., 2011). Des techniques de réduction de dimension, comme l'analyse en composantes principales, isolent les axes comportementaux dominants tout en réduisant le bruit. La reconnaissance de formes basée sur les réseaux constitue un levier supplémentaire. L'analyse des réseaux sociaux (SNA) cartographie les relations indirectes entre acteurs. Des métriques comme la centralité de l'intermédiarité mettent en évidence les comptes intermédiaires servant à relier des sous-réseaux et à dissimuler des flux de superposition (Shaikh et al., 2021). Le couplage des sorties SNA avec des scores d'anomalie permet de contextualiser les alertes individuelles dans des structures plus larges, crucial pour l'étude des collusions et des flux en miroir. L'exploitation de motifs temporels et séquentiels identifie des cycles récurrents de structuration et de transfert offshore, difficilement capturables par de simples seuils. L'intégration de flux d'intelligence externes améliore la précision. Les mises à jour provenant d'unités de renseignement financier via des canaux sécurisés comme Egmont Secure Web ajustent en direct les paramètres de détection (Quintel, 2022). L'analyse des médias défavorables enrichit l'alerte précoce, par exemple lorsque des entités apparaissent dans des rapports négatifs liés au blanchiment. Ces systèmes nécessitent des boucles de rétroaction continues : chaque alerte confirmée ou rejetée alimente les ensembles de réentraînement, réduisant progressivement les

faux positifs (Bakry et al., 2024). Le déploiement opérationnel doit concilier puissance analytique et efficacité informatique, notamment dans les environnements bancaires à forte volumétrie. Les frameworks de traitement de flux permettent une évaluation quasi temps réel, tandis que des routines nocturnes explorent des anomalies émergentes. Des architectures hybrides répartissent les ressources de calcul selon la criticité des segments. L'intégration au sein d'un système de gestion des règles métiers assure une opérationnalisation rapide des modèles détectés (Palakurti, 2023).

Dans le contexte de BGFIBANK Congo, marqué par les flux transfrontaliers liés aux industries extractives, l'usage intensif du cash et la montée des canaux numériques, cette combinaison de détection statistique, d'analyses comportementales et de réseaux est essentielle pour contrer des menaces telles que le blanchiment fondé sur le commerce (Godefroy et al., 2011). Avec une gouvernance transparente, des validations régulières et l'intégration active dans les écosystèmes de renseignement, les banques peuvent transformer des infrastructures statiques en systèmes analytiques dynamiques capables de perturber durablement les flux illicites malgré la complexité et l'échelle des risques (Ryder, s.d.).

3. Mesures procédurales et organisationnelles

a. KYC et diligence renforcée (EDD)

Les procédures KYC établissent l'identité client, incluant informations personnelles, statut juridique, bénéficiaires effectifs (Utkina et al., 2023). Pour les clients à haut risque (PPE, industries extractives, structures opaques), l'EDD exige des vérifications approfondies :

- source des fonds et de la richesse,
- recoupement avec registres internationaux,
- vérifications de terrain lorsque possible (Helgesson & Mörth, 2018).

Tableau 3: Les processus KYC (Know Your Customer) constituent la première barrière procédurale contre l'infiltration de

Étapes du processus KYC	Exigences clés	Outils et sources de vérification	Références
Identification initiale	Collecte des PII (noms légaux, pseudonymes, date et lieu de naissance, N° d'enregistrement pour personnes morales, adresses opérationnelles)	Registres nationaux, listes de surveillance internationales	Utkina et al. (2023)
Vérification documentaire	Validation des données fournies, cohérence avec registres officiels	Documents d'identité, registres de commerce, attestations notariées	Helgesson & Mörth (2018)
Évaluation du risque client	Classification selon profil, secteur, juridiction, flux transfrontaliers	Principes GAFI, scoring de risque	Godefroy et al. (2011)
Due diligence renforcée (EDD)	Vérification des bénéficiaires effectifs, origine des fonds, gouvernance et exposition sectorielle (ex. industries extractives, ONG en zones de conflit)	Déclarations financières, registres internationaux, enquêtes indépendantes, visites sur site	Ryder (s.d.), Akinteye et al. (2023)
Contrôle des flux commerciaux	Détection de la sous/surfacturation, validation des relations contractuelles	Documentation douanière, prix de marché, confirmation via banques correspondantes	Helgesson & Mörth (2018)
Surveillance continue	Rafraîchissement périodique des données KYC, déclencheurs dynamiques en cas de changements	Systèmes BRMS, alertes automatiques, bases de données commerciales	Palakurti (2023), Helgesson & Mörth (2018)

	(actionnariat, activité, flux géographiques)		
Cas spécifiques à haut risque	Clients PPE, correspondents bancaires (KYCC), ONG, entreprises à forte intensité de liquidités	Vérification gouvernance, audits indépendants, Egmont Secure Web	Godefroy et al. (2011), Quintel (2022)
Appui technologique	Signalement automatique des incohérences, détection d'anomalies	IA/ML, systèmes de gestion des règles	Palakurti (2023)
Ressources humaines	Formation spécialisée des équipes KYC/EDD sur les typologies locales et internationales	Formations CRF, orientations GAFI, audits internes	Helgesson & Mörth (2018), Akinteye et al. (2023)
Gouvernance et supervision	Séparation entre fonctions commerciales et conformité, audit interne, escalade au conseil d'administration	Politiques RH, comités de gestion des risques	McConnell (2020)
Coopération externe	Partage d'informations transfrontalières, validation des données hors juridiction	Egmont Secure Web, CRF homologues	Quintel (2022)

La République du Congo, avec ses exportations minières et flux transfrontaliers, impose une vigilance accrue sur la sous-facturation et les intermédiaires offshore (Akinteye et al., 2023).

b. Formation et sensibilisation du personnel

Développer une culture de vigilance contre le blanchiment d'argent et le financement du terrorisme (LBC/FT) repose sur les connaissances, compétences et la conscience situationnelle du personnel. Les contrôles technologiques (section 6.2.1) exigent l'appui humain pour la configuration, l'interprétation et l'action. La formation ne doit pas être un exercice ponctuel de conformité, mais un processus continu, adapté aux évolutions réglementaires et aux typologies émergentes. Les employés en contact client doivent savoir repérer les signaux d'alarme dès l'intégration, comme des incohérences entre déclarations et documents, ou des comportements révélant des financements opaques (Akinteye et al., 2023). Cette compétence est critique dans les économies à forte utilisation d'espèces, où les dépôts structurés imitent l'activité commerciale normale (Utkina et al., 2023). Des études de cas fournies par les cellules de renseignement financier (Helgesson & Mörth, 2018) illustrent comment des transactions routinières peuvent masquer des risques. Les analystes conformité doivent maîtriser les techniques d'enquête avancées, comprendre les scores d'anomalie et les paramètres sectoriels ou géographiques qui guident la priorisation (Palakurti, 2023). Cette capacité permet de challenger les résultats automatisés plutôt que de les accepter passivement, réduisant les risques liés aux limites des algorithmes (Paul et al., 2023).

Une formation spécialisée est nécessaire pour les catégories à haut risque : personnes politiquement exposées, correspondants bancaires, clients du commerce dans les secteurs extractifs, ou ONG opérant en zones de conflit (Godefroy et al., 2011 ; Ryder, s.d.). Les exercices pratiques doivent couvrir la vérification transfrontalière via registres des sociétés et documents douaniers (Helgesson & Mörth, 2018), l'analyse de la gouvernance des ONG et l'identification des structures imbriquées (Akinteye et al., 2023). Les simulations de scénarios renforcent l'aptitude à traiter rapidement des enquêtes complexes. L'intégration des échecs passés nourrit aussi l'apprentissage : par exemple, les cas où l'audit manquait d'indépendance et marginalisait la conformité illustrent la nécessité d'escalader les risques jusqu'aux comités de direction (McConnell, 2020). Des ateliers basés sur des sanctions internationales montrent les conséquences de la non-actualisation des systèmes (Akinteye et al., 2023). Pour BGFIBANK Congo, la formation doit couvrir les vulnérabilités propres à chaque canal : agences, mobile banking (Arim & Wamema, 2022), corridors commerciaux. Les équipes mobiles doivent comprendre les risques de collusion entre agents et les réseaux de transfert détournés (Yang, 2018), tandis que les agents de financement du commerce doivent reconnaître la manipulation des prix (Godefroy et al., 2011). Les programmes doivent être dynamiques : des sessions annuelles sont minimales, mais le rythme de mutation des typologies impose des modules courts de micro-apprentissage intégrés aux systèmes,

avec rappels contextuels lors des saisies de transactions. Les évaluations doivent mesurer non seulement la participation, mais aussi l'impact opérationnel, par exemple via la qualité des dossiers KYC ou des STR. L'efficacité doit être vérifiée par des audits indépendants (Akinteye et al., 2023).

La coopération externe enrichit les programmes : séminaires avec régulateurs, débriefings des forces de l'ordre, échanges au sein du Groupe Egmont (Godefroy et al., 2011 ; Quintel, 2022). L'alignement des incitations est aussi crucial : intégrer des critères LBC/FT dans les évaluations de performance évite de récompenser les seuls résultats commerciaux (McConnell, 2020).

En définitive, la formation du personnel réduit les faux négatifs, améliore la rapidité et la qualité des STR, et permet des ajustements proactifs. Reliée aux cadres de gouvernance et aux technologies adaptatives (Palakurti, 2023), elle transforme les ressources humaines en atout central d'une posture LBC/FT robuste, adaptée à l'environnement spécifique de BGFIBANK Congo.

c. Intégration des approches : du typologique au technologique

L'efficacité de la LCB/FT réside dans la convergence des analyses typologiques et des systèmes de détection. Par exemple :

- Les schémas de **superposition** décrits dans la section 2 trouvent une traduction directe dans les mesures de centralité détectées par la SNA.
- Le **TBML** requiert l'intégration de modules sectoriels corrélant valeurs de factures, prix du marché et flux douaniers (Godefroy et al., 2011).
- Les **sociétés écrans** peuvent être identifiées par reconnaissance de motifs structurels et relations croisées entre administrateurs (Shaikh et al., 2021).

L'environnement opérationnel de BGFIBANK Congo illustre la nécessité d'une approche adaptée : forte intensité de cash, dépendance aux exportations minières, corridors régionaux instables. La combinaison de la cartographie géographique, de l'IA, des audits internes et de la coopération internationale apparaît comme le modèle optimal.

Le blanchiment de capitaux et le financement du terrorisme exploitent la complexité du commerce, l'opacité des structures juridiques et les failles réglementaires. Les institutions financières, particulièrement dans les environnements fragiles comme la République du Congo, doivent conjuguer vigilance humaine et outils technologiques avancés. La complémentarité entre typologies criminelles et systèmes de surveillance technologique offre une capacité proactive de détection et de prévention.

En définitive, l'innovation technologique (IA, big data, analyse des réseaux), couplée à une gouvernance solide et à une coopération interinstitutionnelle, constitue la voie la plus prometteuse pour réduire durablement la vulnérabilité des systèmes financiers face aux menaces du BA/FT.

PARTIE II – Diagnostic du dispositif LCB-FT de BGFIBANK Congo

Chapitre 5 – Analyse contextuelle de BGFIBANK Congo

Introduction du chapitre

Afin d'évaluer de manière rigoureuse le dispositif de détection des transactions suspectes en vigueur au sein de BGFIBANK Congo, il est essentiel de comprendre le cadre institutionnel dans lequel la banque évolue. Ce chapitre présente l'historique, la structure organisationnelle, le positionnement stratégique, ainsi que les outils technologiques mobilisés par l'établissement en matière de conformité. Ces éléments constituent le socle sur lequel sera fondée l'analyse diagnostique approfondie menée dans les chapitres suivants.

1. Aperçu de l'organisation

a. Contexte historique et développement

BGFIBANK Congo est une filiale du Groupe BGFIBank, un acteur bancaire panafricain de référence fondé en 1971 à Libreville, au Gabon. À l'origine établissement public, la Banque Gabonaise et Française Internationale (BGFI) s'est progressivement transformée en groupe bancaire à capital privé majoritairement africain. Cette évolution stratégique a été marquée par une volonté affirmée de modernisation, de professionnalisation de la gouvernance, et d'expansion régionale. Le groupe a ainsi progressivement étendu ses activités au sein de la Communauté Économique et Monétaire de l'Afrique Centrale (CEMAC), en Afrique de l'Ouest, en Afrique de l'Est et jusqu'en Europe, avec des implantations en France et au Portugal.

Dans ce contexte d'expansion régionale, la filiale congolaise a vu le jour en 2002, à Brazzaville, avec pour ambition de répondre aux besoins spécifiques du marché bancaire congolais, alors en pleine recomposition post-crise. Dès sa création, BGFIBANK Congo s'est positionnée comme un établissement de proximité, alliant rigueur financière, innovation technologique et accompagnement du développement économique local. La banque a bénéficié de l'expertise technique et du capital institutionnel du Groupe BGFIBank, tout en adaptant ses pratiques aux réalités du contexte congolais. Au fil des années, BGFIBANK Congo a connu une croissance soutenue, consolidant sa position dans un marché bancaire fortement concentré. Elle est aujourd'hui considérée comme l'un des trois principaux établissements financiers du pays, en termes de total bilan, de volume d'encours, et de nombre de clients actifs. Sa montée en puissance a été favorisée par sa capacité à financer de grands projets d'infrastructure (routes, énergie, BTP), à accompagner les opérateurs économiques stratégiques (secteurs pétrolier, logistique, commerce), et à proposer des produits adaptés aux besoins des entreprises et des particuliers.

Par ailleurs, la banque s'est distinguée par sa résilience face aux chocs économiques (notamment la chute des prix du pétrole en 2014-2016), grâce à une gestion prudente des risques, un dispositif de gouvernance renforcé et un appui stratégique constant du Groupe. Cette solidité s'est traduite par une forte croissance de ses encours, une diversification de ses revenus et une amélioration de sa rentabilité opérationnelle. En 2023, BGFIBANK Congo a également été reconnue pour la qualité de son engagement sociétal et son implication dans des initiatives de financement responsable, notamment à travers son soutien aux PME, aux initiatives de bancarisation et à l'éducation financière.

b. Gouvernance et structure d'entreprise

BGFIBANK Congo s'inscrit dans une gouvernance d'ensemble coordonnée par le Groupe BGFIBank, qui joue un rôle de pilotage stratégique, de supervision des risques et de diffusion des meilleures pratiques au sein de ses différentes filiales. Cette gouvernance est formalisée à travers un dispositif institutionnel structuré, garantissant cohérence, conformité et alignement des politiques internes aux

exigences régionales et internationales. Le Groupe BGFIBank a mis en place un Centre Régional de Conformité (CRC) basé à Libreville, qui centralise les fonctions transversales de conformité pour l'ensemble des filiales de la sous-région CEMAC. Ce centre a pour principales missions :

- La diffusion de directives harmonisées en matière de LCB-FT, de protection des données et de gestion des risques réglementaires ;
- La supervision des dispositifs de conformité à travers des missions d'audit transversal ;
- L'organisation de revues thématiques trimestrielles sur des sujets émergents (crypto-actifs, fintech, sanctions internationales) ;
- L'élaboration de guides de bonnes pratiques et de matrices de risques sectoriels, à destination des filiales ;
- L'accompagnement des équipes locales dans la réponse aux inspections réglementaires menées par la COBAC, l'ANIF ou d'autres autorités nationales.

BGFIBANK Congo bénéficie également du soutien de la Direction Groupe des Risques et Conformité, qui fixe les orientations stratégiques en matière de gouvernance réglementaire. Cette direction pilote les évolutions de la cartographie des risques, la définition des seuils de tolérance, et l'actualisation des politiques KYC (Know Your Customer), CDD (Customer Due Diligence), et EDD (Enhanced Due Diligence). La gouvernance groupe favorise également la montée en compétences par la BGFI Business School, organisme interne de formation professionnelle certifié, qui propose des modules obligatoires et spécialisés dans le domaine de la conformité. En 2023, plus de 2 400 heures de formation ont été dispensées aux collaborateurs des filiales sur les thématiques LCB-FT, protection des données et éthique bancaire. La supervision du dispositif de conformité groupe est assurée par un Comité Groupe de Conformité, qui se réunit chaque trimestre. Ce comité établit un suivi consolidé des indicateurs de risque, vérifie la bonne application des recommandations émises par les autorités de tutelle, et statue sur les priorités d'investissement dans les outils de surveillance.

L'organisation interne de BGFIBANK Congo repose sur une structure fonctionnelle centralisée, conforme aux standards de gouvernance définis par le Groupe BGFIBank. Cette organisation vise à garantir la clarté des responsabilités, la maîtrise des risques et la transversalité des fonctions de contrôle, notamment en matière de conformité LCB-FT. L'architecture de gouvernance se distingue par une articulation équilibrée entre les fonctions commerciales, les fonctions support, et les lignes de contrôle interne. Le schéma organisationnel s'articule autour de la Direction Générale, placée sous la supervision du Conseil d'Administration. La Direction Générale est assistée de plusieurs directions exécutives et opérationnelles, parmi lesquelles :

- La Direction de la Conformité et du Contrôle Permanent, chargée de la supervision des dispositifs de vigilance LCB-FT, du contrôle interne de niveau 2, et du suivi des obligations réglementaires ;
- La Direction des Risques, responsable de l'identification, l'évaluation et la mitigation des risques de crédit, de marché, opérationnels et de réputation ;
- La Direction de l'Audit Interne, qui exerce une fonction de contrôle de niveau 3 en toute indépendance, rattachée directement au Conseil d'Administration ;
- La Direction Commerciale, subdivisée en pôles spécialisés : Banque de détail, Banque des entreprises, Services bancaires spécialisés ;
- La Direction des Systèmes d'Information et du Digital, en charge de l'architecture technologique, de la sécurité des données, et des projets d'automatisation.

Ainsi, le dispositif de gouvernance de la conformité au sein de BGFIBANK Congo comprend un organe central dédié à la lutte contre le blanchiment de capitaux et le financement du terrorisme : le Comité LCB-FT. Ce comité interne, institué par décision de la Direction Générale, incarne la volonté de l'établissement de renforcer la coordination, la supervision et le suivi stratégique des actions de conformité, conformément aux exigences de la COBAC (Instruction n°01/2019/LCB-FT) et aux standards internationaux du GAFI.

Le Comité LCB-FT se réunit mensuellement, ou à tout moment en session extraordinaire en cas de signalement critique. Il est présidé par le Chief Compliance Officer (CCO), qui en assure l'animation et

fixe l'ordre du jour en lien avec les risques identifiés. Le comité est composé de membres permanents et de membres invités selon les thématiques abordées.

Les membres permanents sont :

- Le Chief Compliance Officer (président du comité)
- Le Directeur Juridique
- Le Responsable de la Sécurité Financière
- Un représentant de l'Audit Interne
- Un représentant de la Direction des Risques
- Un analyste conformité senior (secrétariat du comité)

Les membres invités peuvent inclure : le Responsable des Opérations, le Directeur Commercial, le Responsable IT, ou tout cadre impliqué dans un cas spécifique ou dans un projet de transformation lié à la conformité.

Les principales attributions du comité sont les suivantes :

- Valider et suivre les alertes LCB-FT générées par le système SAP AML Watch ;
- Statuer sur les dossiers d'opérations douteuses (DOD) à transmettre à l'ANIF, selon une grille d'analyse multicritères ;
- Suivre les plans d'action correctifs en matière de conformité, notamment suite aux audits internes ou aux missions de la COBAC ;
- Superviser les évolutions technologiques ou organisationnelles relatives aux dispositifs LCB-FT (intégration de nouveaux modules, renforcement des seuils d'alerte, automatisation des reportings) ;
- Évaluer les profils de risque client à partir des indicateurs consolidés (KYC, typologies, historique d'anomalies).

En pratique, les travaux du comité donnent lieu à la rédaction de procès-verbaux formels, archivés de manière sécurisée, et accessibles à la Direction Générale, au Conseil de Surveillance et, le cas échéant, aux autorités de supervision. Le Comité LCB-FT constitue ainsi un levier essentiel de gouvernance opérationnelle et stratégique. Il permet à la banque d'adapter rapidement sa vigilance face à l'évolution des menaces, d'aligner les différentes fonctions internes autour d'une approche intégrée du risque, et d'assurer une traçabilité rigoureuse des décisions en matière de conformité.

c. Modèle d'affaires et position sur le marché

Dans un paysage bancaire congolais encore marqué par une forte concentration des acteurs et une bancarisation limitée (estimée à environ 15 % de la population adulte selon la BEAC, 2023), BGFIBANK Congo occupe une place stratégique. En moins de deux décennies, elle s'est hissée parmi les trois premières banques du pays, rivalisant avec des institutions à capitaux majoritairement internationaux. Cette position s'explique par une politique de croissance soutenue, un ancrage local fort et un positionnement différencié sur des segments stratégiques.

Au 31 décembre 2024, selon les données consolidées de la COBAC et du Rapport annuel du Groupe BGFIBank (2023), la filiale congolaise représentait :

- 17,4 % des encours de crédit du secteur bancaire congolais, en grande partie orientés vers le financement des grandes entreprises et des infrastructures
- 21,6 % des dépôts globaux, démontrant la confiance des particuliers, entreprises et institutions dans la solidité de la banque
- Plus de 150 000 clients actifs, dont environ 12 % sont des PME/PMI, 2 % des grandes entreprises, et 86 % des clients particuliers

BGFIBANK Congo joue ainsi un rôle moteur dans le financement de l'économie nationale. Elle est particulièrement présente dans les secteurs jugés prioritaires pour la croissance du pays : pétrole, BTP, logistique, commerce de gros, télécommunications et services publics. Son portefeuille est structuré à

hauteur de 60 % autour des grands comptes et projets structurants, tandis que les 40 % restants concernent les segments retail et PME.

Par ailleurs, la banque a su diversifier ses sources de revenus, en développant notamment des lignes métiers comme la gestion de patrimoine, la banque transactionnelle, le financement du commerce et la monétique. Elle s'est également positionnée comme acteur innovant dans le développement des produits digitaux, devenant ainsi l'une des premières banques à proposer des services de mobile banking, de wallet interopérable et de crédit instantané digitalisé.

Cette dynamique d'expansion se traduit aussi par une présence physique croissante : BGFIBANK Congo dispose actuellement de 11 agences réparties entre Brazzaville, Pointe-Noire et Dolisie, complétées par un réseau de guichets automatiques (GAB) et une plateforme e-banking en constante amélioration.

Enfin, l'établissement se distingue par ses résultats financiers solides, avec un résultat net en hausse de 12 % en 2023, et une croissance moyenne annuelle de son portefeuille crédit de 8 % sur les cinq dernières années. Ce dynamisme fait de BGFIBANK Congo un acteur incontournable de la stabilité financière et du financement du développement en République du Congo.

d. Relations avec les autorités

BGFIBANK Congo entretient des relations suivies avec l'Agence Nationale d'Investigation Financière (ANIF) :

- Transmission mensuelle des DOD et des indicateurs AML
- Participation à des inspections ponctuelles (deux contrôles en 2023)
- Échange encore insuffisant sur les retours d'expérience ou cas complexes

Des efforts de coordination restent nécessaires pour instaurer une boucle d'amélioration continue entre les établissements déclarants et l'autorité centrale.

L'établissement est engagé dans plusieurs initiatives :

- Partenariat avec MTN Congo pour la sécurisation des flux mobile money
- Projet pilote avec une fintech française pour développer un algorithme de "Risk Scoring KYC" (en phase de test)
- Membre du réseau bancaire CEMAC LCB-FT, piloté par la COBAC

2. Environnement opérationnel

a. Secteur bancaire en République du Congo

Le secteur bancaire de la République du Congo fonctionne dans un cadre influencé à la fois par les priorités réglementaires nationales et par les structures économiques régionales plus larges, façonnées en partie par l'adhésion à la Communauté économique et monétaire de l'Afrique centrale (CEMAC) avec sa banque centrale commune, la Banque des États de l'Afrique centrale (BEAC). La composition du secteur comprend un mélange de banques locales, de filiales de groupes financiers étrangers et d'institutions de microfinance, toutes au service d'une économie caractérisée par une dépendance concentrée aux exportations de pétrole, un segment important du marché informel et d'importantes populations sous-bancarisées. Ce contexte structurel influence les cycles de liquidité, l'exposition au risque de crédit et les modèles d'intermédiation financière, tout en présentant des défis notables pour l'application de la loi en matière de lutte contre le blanchiment d'argent et le financement du terrorisme. Le taux de pénétration des services bancaires formels reste relativement faible par rapport aux moyennes régionales ou mondiales. L'utilisation massive d'argent liquide est généralisée en raison de limitations infrastructurelles telles que la couverture insuffisante des agences rurales et les faibles niveaux d'intégration entre les banques et les mécanismes d'épargne informels. Ces conditions créent des

vulnérabilités qui peuvent être exploitées pour superposer des étapes de blanchiment d'argent par le biais d'entreprises à forte intensité de liquidités ou de la conversion rapide de la monnaie physique en dépôts formels sans justification économique claire (Utkina et al., 2023). Ces dernières années, les campagnes de propriété de comptes promues par les autorités réglementaires visant à renforcer l'inclusion financière ont été progressivement développées, mais l'extension des canaux d'accès, via des intégrations bancaires mobiles ou des modèles d'agents bancaires, introduit une complexité parallèle à la conformité AML/CTF lorsque les systèmes de surveillance des transactions ne sont pas adaptés aux environnements de transfert à volume élevé et de faible valeur (Palakurti, 2023). Le contrôle institutionnel incombe principalement à la BEAC pour la régulation prudentielle et la politique monétaire, complété au niveau national par des structures du ministère des Finances en coordination avec les divisions de surveillance chargées de veiller au respect des dispositions du droit bancaire. En conséquence, la supervision LBC/FT implique à la fois des inspections sur place et l'analyse hors site des rapports déposés auprès de la Cellule de renseignement financier (CRF) du pays. Cependant, des lacunes en matière de capacités opérationnelles, allant de ressources humaines qualifiées à des technologies de détection avancées, persistent dans toutes les parties du secteur, ce qui crée une application inégale des mesures préventives, même parmi les banques officiellement agréées (Akinteye et al., 2023). Cela peut conduire à un arbitrage réglementaire si les entités estiment que l'application de la loi est plus clémente localement que dans les juridictions voisines de la CEMAC. Le paysage bancaire congolais est également fortement influencé par les flux commerciaux transfrontaliers avec les partenaires régionaux, en particulier le Gabon, le Cameroun et la République démocratique du Congo, et par le commerce maritime via Pointe-Noire. Cette dynamique commerciale amplifie l'exposition aux stratagèmes de blanchiment d'argent fondés sur le commerce, où les biens sont mal évalués ou les volumes mal déclarés pour transférer secrètement la valeur d'une juridiction à l'autre (Godefroy et coll., 2011). Pour être efficace, l'atténuation nécessite une coopération étroite entre les autorités douanières et les équipes de financement du commerce des banques afin d'examiner les crédits documentaires au-delà des contrôles de conformité de base. Pourtant, l'alignement entre ces organismes varie dans la pratique en raison des différences dans les mandats institutionnels et les protocoles d'échange d'information. La performance macroéconomique affecte la stabilité du système par l'impact de la volatilité des revenus pétroliers sur la solvabilité du secteur public et la liquidité des devises. La baisse des prix du pétrole peut réduire les réserves de change disponibles pour le règlement interbancaire et entraîner un resserrement des conditions de prêt. Les contractions économiques peuvent faire baisser la demande de prêts formels, mais paradoxalement augmenter les flux illicites associés à la contrebande ou aux canaux d'exportation informels, car les acteurs recherchent d'autres sources de revenus, des flux qui peuvent recouper des transactions bancaires via des dépôts de sociétés écrans ou d'intermédiaires conçus pour masquer la propriété effective (Helgesson & Mörth, 2018). Dans de tels environnements, la pression commerciale exercée sur les banques pour maintenir le volume des transactions doit être soigneusement équilibrée avec les risques élevés de conformité. Dans le domaine de la réglementation, l'intégration des exigences alignées sur le GAFI dans les législations nationales a progressé, mais se heurte à des défis liés à une mise en œuvre proportionnée dans un secteur relativement petit. Les entités assujetties sont tenues de procéder à une vigilance à l'égard de la clientèle, de surveiller les comptes pour détecter les activités suspectes, de conserver les données transactionnelles pendant les périodes légales et de soumettre rapidement les déclarations d'opérations suspectes à la CRF (Akinteye et al., 2023). Alors que les grandes filiales de groupes internationaux disposent généralement de services de conformité structurés et alignés sur les politiques à l'échelle du groupe, les petites institutions manquent parfois d'unités dédiées à la lutte contre le blanchiment d'argent ou s'appuient excessivement sur des processus d'examen manuels susceptibles d'erreurs de surveillance (McConnell, 2020).

b. Environnement réglementaire et autorités de surveillance

L'architecture réglementaire de la République du Congo (Congo-Brazzaville) en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT) repose sur une combinaison de dispositifs communautaires hérités de son appartenance à la Communauté Économique et Monétaire de l'Afrique Centrale (CEMAC) et de structures nationales chargées d'assurer la supervision opérationnelle. Au cœur de ce système, la Banque des États de l'Afrique Centrale (BEAC) assume le

rôle d'autorité monétaire commune, garantissant la stabilité du système bancaire et édictant les règlements prudentiels en coordination avec la Commission Bancaire de l'Afrique Centrale (COBAC), qui agit comme régulateur prudentiel primaire des établissements de crédit agréés (Banque mondiale, 2022). La COBAC est dotée de pouvoirs d'inspection sur place et hors site visant à vérifier la conformité des banques et institutions de microfinance aux normes prudentielles, aux obligations de vigilance client et aux procédures de signalement des transactions suspectes.

À l'échelle nationale, la Cellule nationale de traitement des informations financières (CENTIF-Congo), créée par la loi n°37-2009, joue un rôle central. Organisme autonome rattaché au ministère des Finances, elle est chargée de recevoir, analyser et diffuser les déclarations d'opérations suspectes (DOS) émanant des institutions financières et des entités assujetties non financières. Elle conduit des analyses opérationnelles pour identifier des cas individuels de blanchiment et des analyses stratégiques visant à déceler des tendances émergentes dans des secteurs vulnérables, tels que le négoce de ressources naturelles, la corruption dans les marchés publics ou les flux transfrontaliers d'espèces (GIABA, 2021). La CENTIF dispose de pouvoirs d'accès aux bases de données administratives, de demande d'informations complémentaires et de transmission de dossiers au parquet lorsque des infractions sous-jacentes sont établies. L'ossature réglementaire congolaise s'appuie sur les directives et règlements de la CEMAC transposant les recommandations du Groupe d'Action Financière (GAFI). Ces textes codifient les obligations préventives relatives à l'identification et à la vérification des clients, au contrôle des bénéficiaires effectifs, à la conservation des documents et à la déclaration des opérations douteuses, même lorsqu'elles n'aboutissent pas. Ils incluent également des adaptations liées au caractère informel et très liquide de l'économie congolaise, notamment par la fixation de seuils de vigilance renforcée pour les dépôts en espèces de grande valeur (Banque africaine de développement, 2020). La coordination interinstitutionnelle s'opère à travers le Comité national de lutte contre le blanchiment de capitaux et le financement du terrorisme, chargé d'harmoniser les politiques entre la Banque centrale, la COBAC, la CENTIF et les ministères de tutelle couvrant les professions non financières désignées (notaires, casinos, négociants en pierres précieuses, agents immobiliers). Toutefois, comme l'ont souligné des évaluations du GIABA, l'efficacité de ce dispositif reste conditionnée à une meilleure allocation des ressources humaines et techniques, ainsi qu'à une coopération fluide entre autorités judiciaires et régulateurs (GIABA, 2021).

Enfin, l'insertion du Congo-Brazzaville dans les réseaux régionaux et internationaux de coopération est déterminante. En tant qu'État membre de la CEMAC et participant aux travaux du GIABA en tant qu'observateur, le pays bénéficie d'échanges typologiques et de l'utilisation de plateformes comme l'Egmont Secure Web pour les transmissions de renseignements financiers transfrontaliers (Egmont Group, 2022). Néanmoins, des défis persistent, liés notamment aux écarts de confidentialité entre législations nationales partenaires et aux limites de capacités locales pour exploiter efficacement les technologies de détection. Dans ce contexte, l'appui technique d'organismes internationaux constitue un levier essentiel pour renforcer l'efficacité du régime national LBC/FT et garantir sa crédibilité auprès des contreparties financières mondiales.

Chapitre 6 – Méthodologie d'évaluation

Introduction du chapitre

L'évaluation du dispositif de détection des transactions suspectes au sein de BGFIBANK Congo repose sur une démarche méthodologique rigoureuse, pensée pour concilier l'exigence académique d'une recherche qualitative approfondie et la nécessité pratique d'analyser les dynamiques concrètes de conformité à la lutte contre le blanchiment de capitaux et le financement du terrorisme (LCB-FT). Cette étude s'inscrit dans un contexte institutionnel marqué par des contraintes fortes, où les banques congolaises évoluent dans un environnement réglementaire régional structuré par la COBAC et la BEAC, et soumis aux standards du GAFI. Comprendre comment une institution financière telle que BGFIBANK Congo met en œuvre ses obligations LCB-FT suppose non seulement une lecture des textes et recommandations, mais aussi une immersion dans ses pratiques internes, ses contraintes organisationnelles et les perceptions de ses acteurs de première ligne.

Ce chapitre méthodologique explicite les fondements de la recherche, justifie le recours à une approche qualitative et présente en détail les outils de collecte et de traitement des données. L'analyse combine ainsi trois axes : les sources documentaires internes et externes, les entretiens semi-directifs menés avec les acteurs clés de la banque, et la construction d'une grille d'évaluation multicritères permettant de positionner le dispositif sur une échelle de maturité. À travers cette combinaison, la méthodologie retenue vise à croiser les règles formelles et les pratiques effectives, à mettre en lumière les écarts entre conformité normative et efficacité opérationnelle, et à proposer une lecture critique des forces et faiblesses du système.

1. Approche méthodologique générale

a. Nature de la recherche

La présente recherche adopte une approche qualitative exploratoire et diagnostique. Le choix d'une démarche qualitative s'impose en raison de la nature du phénomène étudié : la détection des transactions suspectes n'est pas seulement une question technique, mais aussi une pratique organisationnelle façonnée par des interactions humaines, des arbitrages entre impératifs réglementaires et commerciaux, et une culture de conformité propre à chaque institution. Les chiffres bruts (nombre d'alertes, pourcentage de faux positifs, volumes de DOD) fournissent une information utile, mais insuffisante pour comprendre en profondeur les mécanismes qui structurent la détection. Seule une analyse qualitative permet d'appréhender les logiques internes, les contraintes ressenties par les équipes, les blocages communicationnels et la perception des acteurs de terrain.

Cette recherche s'inscrit donc dans une perspective exploratoire visant à comprendre les dynamiques internes du dispositif LCB-FT, mais aussi diagnostique dans la mesure où elle cherche à identifier les écarts entre prescriptions théoriques et réalités pratiques afin de dégager des pistes d'optimisation. Le choix du cas unique – BGFIBANK Congo – se justifie par la volonté d'approfondir un terrain précis plutôt que de disperser l'analyse. Dans les sciences de gestion et en matière de conformité, l'étude de cas unique permet de produire une connaissance riche, contextualisée et transposable sous certaines conditions à d'autres institutions évoluant dans des environnements similaires.

b. Justification du choix méthodologique

Le recours à une méthodologie qualitative se justifie par plusieurs raisons.

Premièrement, la détection des transactions suspectes est un processus fortement influencé par les pratiques humaines, la collaboration inter-départements et la subjectivité des interprétations. Une

approche quantitative pure ne pourrait pas capturer les nuances, les tensions et les perceptions des acteurs.

Deuxièmement, le sujet de recherche touche à des aspects sensibles de conformité et de gouvernance où l'accès aux données est limité : la transparence est plus facilement obtenue à travers des entretiens confidentiels qu'à travers des bases de données quantitatives exhaustives.

Troisièmement, une démarche qualitative permet d'intégrer des sources variées (documents, entretiens, observations indirectes) et de procéder à une triangulation des informations pour renforcer la validité des résultats.

En outre, l'approche qualitative permet de confronter la norme au réel. Par exemple, la COBAC fixe des règles de vigilance et de détection, mais la manière dont celles-ci sont appliquées au quotidien dépend des ressources disponibles, de la technologie utilisée et de la culture interne. Seule une analyse qualitative permet de mettre en évidence ces écarts, d'identifier les sources de dysfonctionnement et de comprendre les marges de manœuvre des acteurs.

Enfin, cette démarche offre la flexibilité nécessaire pour explorer de nouvelles thématiques émergentes, comme le recours à l'intelligence artificielle dans la détection ou les tensions entre conformité et objectifs commerciaux.

c. Sources documentaires mobilisées

La méthodologie a mobilisé deux types de sources documentaires : internes et externes. Les documents internes de BGFIBANK Congo ont constitué une base précieuse pour comprendre la structuration du dispositif. Ils incluent les procédures internes de conformité, les rapports d'audit LCB-FT et un registre anonymisé des alertes traitées entre 2022 et 2023. Ces sources permettent d'analyser les flux réels de détection, les recommandations déjà formulées en interne et les tendances dans la gestion des alertes.

Documents internes de BGFIBANK Congo utilisés :

- Procédures internes de conformité
- Rapports d'audit LCB-FT
- Registre des alertes 2022–2023 (version anonymisée)

Les documents externes complètent cette vision en apportant un cadre normatif et comparatif. Il s'agit notamment des rapports annuels de l'Agence nationale d'investigation financière (ANIF), des recommandations et circulaires émises par la COBAC, ainsi que des benchmarks régionaux produits par le GIABA et le GABAC. Ces documents permettent de situer BGFIBANK Congo par rapport à ses obligations légales et aux standards internationaux, mais aussi de comparer son dispositif à celui d'autres institutions de la région. L'usage de sources externes renforce la robustesse de l'analyse en évitant l'écueil d'une vision uniquement interne.

Documents externes utilisés :

- Rapports ANIF (2021–2023)
- Recommandations COBAC
- Benchmark régional GIABA et GABAC`

2. Entretiens semi-directifs

a. Profil des personnes interrogées

Dix entretiens semi-directifs ont été réalisés entre mars et juin 2025. Les profils ont été sélectionnés de manière à couvrir l'ensemble des acteurs impliqués dans la chaîne de détection et de traitement des alertes. Quatre analystes LCB-FT ont été interrogés pour comprendre le cœur du dispositif opérationnel, notamment la gestion quotidienne des alertes et la perception de la charge de travail. Deux responsables conformité, dont le Chief Compliance Officer, ont apporté une vision stratégique et managériale, en insistant sur la robustesse normative et les limites d'efficacité. Deux responsables IT & Data ont été interrogés afin d'analyser les capacités techniques des outils AML et les perspectives d'automatisation.

Enfin, deux gestionnaires de clientèle et un responsable des opérations ont permis de comprendre les interactions entre le département Conformité et les métiers commerciaux ou opérationnels.

Cette diversité de profils garantit une vision complète des processus et met en évidence les zones de tension entre conformité, business et opérations. Les entretiens ont duré en moyenne entre 35 minutes et 50 minutes, selon le profil, et ont été intégralement retranscrits avec l'accord des participants.

Fonction	Nombre d'entretiens	Durée moyenne
Analystes LCB-FT	4	60 min
CCO et Responsable Conformité	2	75 min
IT & Data	2	45 min
Front office (banque entreprise)	2	45 min

b. Thèmes abordés

Le guide d'entretien a été conçu sur la base du questionnaire préparatoire, structuré en six sections :

- Contexte et perception générale du dispositif ;
- Dispositif technologique et évaluation des outils AML (faux positifs, pertinence des scénarios, ergonomie) ;
- Processus organisationnels et humains (traitement des alertes, communication inter-départements, goulots d'étranglement) ;
- Culture et compétences (niveau de formation, adhésion à la conformité, sensibilisation des collaborateurs) ;
- Perspectives d'optimisation (intégration de l'IA, automatisation, recommandations stratégiques) ;
- Évaluation globale de la robustesse du dispositif et facteurs clés de succès.

Ces thématiques permettent d'articuler la recherche entre dimensions techniques, organisationnelles et humaines, conformément aux axes de la grille d'analyse.

c. Modalité de traitement

- Enregistrements (avec accord) + retranscriptions ;
- Analyse thématique assistée via Excel ;
- Codage manuel par mots-clés : faux positifs, charge de travail, filtrage, DOD, outil, communication, ressources, manque d'interconnexion.

3. Construction de la grille d'analyse

Une grille d'évaluation multicritères a été élaborée pour structurer le diagnostic du dispositif LCB-FT. Elle s'inspire des cadres de référence suivants :

- Modèle de maturité LCB-FT du GAFI
- Indicateurs de performance des Big Four (Deloitte, EY)
- Principes de la gestion intégrée des risques (IRM)

a. Dimensions évaluées

Afin de structurer l'évaluation du dispositif LCB-FT, une grille multicritère a été construite en s'inspirant de plusieurs cadres de référence : le modèle de maturité du GAFI, les indicateurs de performance proposés par les Big Four (Deloitte, EY) et les principes de la gestion intégrée des risques (IRM). Cinq dimensions principales ont été retenues :

Domaine	Sous-dimension	Indicateur
Technologie	Performance du système AML	Taux de faux positifs, taux de conversion
Organisation	Gouvernance conformité	Fréquence des comités, niveau d'implication
Processus	Traitement des alertes	Délai moyen de traitement, rétroaction
Humain	Compétences et formation	Certification, heures de formation annuelle
Culture	Adhésion des métiers	Indicateurs de collaboration, remontée d'alertes

Ces dimensions couvrent les aspects techniques, structurels et culturels du dispositif, permettant d'évaluer non seulement sa conformité réglementaire, mais aussi son efficacité opérationnelle et son appropriation par les acteurs.

b. Pondération

Chaque critère est noté sur 5, avec une pondération par domaine :

Domaine	Pondération
Technologie	25 %
Organisation	20 %
Processus	20 %
Ressources humaines	20 %
Culture de conformité	15 %

4. Traitement et analyse des données

a. Analyse qualitative

- Croisement des entretiens avec les procédures internes
- Identification de points de friction entre théorie et pratique
- Triangulation des données pour valider la cohérence

b. Analyse comparative

Les résultats de l'analyse ont été confrontés aux bonnes pratiques identifiées dans la littérature et aux standards internationaux. Une échelle de maturité a été appliquée à BGFIBANK Congo, positionnant son dispositif entre le stade « émergent » et « optimisé », en fonction des dimensions considérées. Par exemple, la gouvernance conformité est relativement robuste grâce à l'implication de la direction

générale, mais la technologie reste limitée par la rigidité des scénarios de détection et la surcharge de faux positifs. De même, la culture de conformité progresse mais demeure encore cantonnée au département Conformité, avec une appropriation inégale par les métiers commerciaux

- Confrontation avec les bonnes pratiques identifiées au chapitre 4
- Positionnement de BGFIBANK Congo sur une échelle de maturité (Initiale – Émergente – Optimisée – Résiliente)

c. Limites méthodologiques

La méthodologie adoptée présente plusieurs limites.

D'abord, l'échantillon d'entretiens reste restreint en raison des contraintes de confidentialité, ce qui limite la représentativité statistique.

Ensuite, l'absence de mesure directe de la perception des clients empêche d'évaluer l'impact externe du dispositif.

Par ailleurs, certaines données IT confidentielles n'ont pas pu être consultées, restreignant l'analyse technologique.

Enfin, le biais de désirabilité sociale peut avoir influencé certaines réponses, malgré les garanties de confidentialité données aux participants. Ces limites n'invalident pas les résultats, mais appellent à les interpréter avec prudence et à les compléter par de futures recherches quantitatives ou comparatives.

Ce chapitre a présenté la méthodologie mise en œuvre pour évaluer le dispositif de détection des transactions suspectes de BGFIBANK Congo. Fondée sur une approche qualitative exploratoire et diagnostique, la recherche a mobilisé des sources documentaires internes et externes, conduit dix entretiens semi-directifs auprès d'acteurs clés, et élaboré une grille multicritère permettant de structurer l'évaluation. Le traitement des données par codage thématique et triangulation a permis de dégager une analyse cohérente, confrontée aux standards internationaux.

Les limites identifiées – taille réduite de l'échantillon, absence de données clients, accès partiel aux outils IT – n'enlèvent pas à la méthodologie sa pertinence pour comprendre les dynamiques internes du dispositif. Le corpus de données recueilli fournit une base solide pour l'analyse critique du chapitre suivant, où seront mises en évidence les forces et faiblesses du système, ainsi que des pistes d'optimisation concrètes.

Chapitre 7 – Analyse et résultats

Introduction du chapitre

Après avoir défini l'environnement institutionnel et réglementaire dans lequel opère BGFIBANK Congo (chapitre 5) puis explicité la méthodologie retenue (chapitre 6), ce chapitre présente les résultats issus de l'analyse qualitative menée. Ceux-ci s'appuient sur la grille multicritère élaborée et sur la triangulation entre sources documentaires internes, rapports externes, entretiens semi-directifs et comparaisons internationales. L'objectif est de dresser un diagnostic complet du dispositif de détection des transactions suspectes, en identifiant les forces structurelles, les faiblesses opérationnelles, les facteurs d'influence internes et externes, et enfin les opportunités d'optimisation. Cette analyse est indispensable pour comprendre où se situe la banque dans son parcours de maturité LCB-FT et quelles sont les conditions de succès pour améliorer son efficience.

1. Forces et avantages compétitifs

a. Une gouvernance structurée et alignée

L'un des principaux atouts mis en évidence est la robustesse de la gouvernance en matière de conformité. BGFIBANK Congo dispose d'un Comité LCB-FT opérationnel qui se réunit mensuellement, assurant un suivi continu des alertes et des risques identifiés.

La présence du Chief Compliance Officer au sein du comité de direction garantit l'indépendance fonctionnelle du dispositif et son alignement stratégique avec les orientations de la banque.

Les entretiens confirment que le soutien de la direction générale est réel et constitue un facteur clé de crédibilité : « La direction générale nous soutient, ce qui est notre plus grande force » confie le responsable conformité. Cet ancrage institutionnel assure que les préoccupations liées à la LCB-FT ne sont pas marginalisées, mais intégrées au cœur des arbitrages stratégiques. L'existence de tableaux de bord et d'outils de reporting vers les lignes métiers illustre également une volonté de rendre la conformité lisible et partagée.

b. Un système AML en place et partiellement automatisé

Sur le plan technologique, BGFIBANK Congo utilise SAP AML Watch, interfacé avec le système bancaire T24. Cet outil assure le filtrage automatisé des listes de sanctions (ONU, OFAC, UE) et génère des alertes selon des seuils et des profils prédéfinis.

Depuis 2022, la déclaration d'opérations douteuses (DOD) à l'ANIF est automatisée, réduisant les délais et minimisant les erreurs humaines.

Le responsable IT/Data confirme que les fondations technologiques sont stables et sécurisées : « Les plateformes supportant la LCB-FT sont opérationnelles et performantes. Le système filtre bien les listes et applique les scénarios qu'on lui donne ».

Cette infrastructure assure la conformité de base et permet d'absorber un volume important de transactions. De plus, les interactions entre IT et conformité sont jugées fluides, garantissant une adaptabilité aux évolutions réglementaires.

c. Un Écosystème Technologique Spécialisé

La banque s'est dotée d'une suite d'outils spécialisés et reconnus (SIRON AML, SIRON KYC, SWIFT Sanction Screening). Cette trinité technologique assure une couverture complète du cycle de vie du risque : au moment de l'entrée en relation (criblage KYC), lors des transactions internationales (filtrage SWIFT) et dans le suivi comportemental continu (surveillance des transactions).

d. Un Engagement Stratégique Fort et Visible

La LCB-FT n'est pas traitée comme une simple obligation réglementaire, mais comme un axe stratégique majeur. La supervision est assurée au plus haut niveau par un Comité des Risques et de la Conformité émanant du Conseil d'Administration, et la "Maîtrise des Risques" est un des cinq piliers du plan d'entreprise "Dynamique 2025". Cet alignement stratégique est une force fondamentale.

e. Un capital humain compétent

BGFIBANK Congo dispose d'une équipe dédiée de quatre analystes AML, tous certifiés COBAC niveau 2. Ces analystes démontrent une bonne maîtrise des procédures, une capacité d'adaptation et un engagement notable malgré une charge de travail élevée.

Les entretiens révèlent leur frustration face aux faux positifs, mais aussi leur professionnalisme et leur volonté d'améliorer le dispositif : « On passerait moins de temps à faire de l'administratif et plus de temps à faire notre vrai métier : l'enquête » affirme un analyste.

Par ailleurs, la collaboration avec l'audit interne et l'IT est jugée constructive, et les métiers commerciaux sont progressivement sensibilisés. Cette combinaison d'expertise technique et d'implication humaine constitue une base solide pour renforcer la maturité du dispositif.

2. Faiblesses et points de friction

a. Taux de faux positifs élevé

Le point de douleur le plus unanimement évoqué est la surproduction d'alertes non pertinentes. Selon les données internes et les témoignages, plus de 90 % des alertes générées ne débouchent pas sur une suspicion réelle.

Le responsable conformité confirme : « Notre outil génère plus de 1200 alertes par mois, et plus de 90 % ne sont pas pertinentes ».

Cette inefficience entraîne une consommation massive de ressources, une démotivation des équipes et un risque accru d'erreurs par lassitude. Les analystes expriment leur frustration face à la répétition d'alertes identiques pour les mêmes clients, faute d'apprentissage dynamique du système.

b. Absence d'analyse comportementale

L'absence d'intelligence artificielle ou de machine learning constitue une faiblesse majeure. Le système repose sur des règles statiques, incapables de détecter des schémas complexes ou évolutifs.

Le responsable conformité insiste : « Ils n'ont pas de capacité d'apprentissage. Un client dont l'activité évolue légitimement peut générer des alertes tous les mois ». L'absence d'analyse comportementale limite la pertinence des détections et creuse l'écart avec les bonnes pratiques internationales.

c. Rétroaction limitée de l'ANIF

Un autre point récurrent est l'absence de retour de l'ANIF sur les DOD transmises. Les analystes et responsables conformité regrettent de travailler dans une « boîte noire » : « On n'a jamais de retour pour savoir si notre dossier a été utile ».

Cette absence de feedback démotive les équipes et réduit l'apprentissage organisationnel. Contrairement à d'autres juridictions où les CRF (cellules de renseignement financier) partagent des statistiques ou des tendances, l'ANIF congolaise n'offre pas de rétroaction systématique.

d. Manque de ressources humaines

L'effectif de quatre analystes, bien que compétents, est insuffisant au regard du volume d'alertes (environ 60 par jour/analyste). Cette surcharge génère fatigue, risque d'erreur et absence de

spécialisation. « Idéalement, j'aimerais avoir un expert sur la fraude documentaire, un autre sur les flux liés au commerce international… Nous n'avons pas le temps pour cette montée en expertise » explique le responsable conformité.

e. Autres points d'analyses

- Les entretiens avec le gestionnaire de clientèle et le manager commercial montrent que les contraintes de conformité sont souvent perçues comme un frein. Le gestionnaire de clientèle parle d'un « obstacle au closing » et souligne que certains clients se plaignent de blocages jugés injustifiés. Cette tension illustre un défi culturel : la conformité est vue comme punitive plutôt que comme un levier de crédibilité. L'absence de communication pédagogique renforce ce malaise.
- Le responsable de l'audit interne insiste sur le caractère « post-événement » de ses missions. L'audit intervient après coup et peine à tester la pertinence des scénarios AML. Cette posture limite l'impact préventif et laisse des zones aveugles dans la surveillance.
- Le responsable des opérations insiste sur la gêne occasionnée pour les clients corporate lors du blocage des virements SWIFT. « Le client attend, et le flux est interrompu ». Ces blocages nuisent à la satisfaction client et peuvent affecter la réputation externe de la banque.
- Plusieurs analystes évoquent un sentiment de lassitude lié au volume d'alertes et au manque de retour. Cette « fatigue de conformité » réduit la motivation et accentue le risque d'erreurs humaines.
- Le responsable IT confirme que SAP AML Watch est robuste mais rigide : « Le système est statique, il ne permet pas d'analyse dynamique ». L'intégration avec T24 ralentit l'évolution des scénarios, empêchant d'innover rapidement.
- Les témoignages convergent sur l'absence de canaux rapides d'escalade entre conformité, opérations et commercial. Le manque de coordination allonge les délais de traitement et fragilise la gestion des cas urgents.

3. Analyse comparative avec les bonnes pratiques internationales

L'analyse comparative révèle un écart notable entre BGFIBANK Congo et les standards des grandes banques internationales. Là où certaines institutions (HSBC, Crédit Agricole) intègrent déjà des moteurs IA/ML capables de contextualiser les alertes, BGFIBANK s'appuie encore sur un système statique.

Les analystes certifiés sont quatre, contre des dizaines dans les banques internationales. L'absence de profil client dynamique, mis à jour automatiquement en fonction des données disponibles, contraste avec les pratiques avancées où les KYC sont vivants et connectés à des sources multiples.

De même, le partage d'informations entre les banques et les CRF reste limité localement, alors que des pays comme la France (TRACFIN) ou le Royaume-Uni (FCA) encouragent un dialogue actif.

Sur l'échelle de maturité, BGFIBANK Congo se situe au stade « intermédiaire-émergent » : une gouvernance solide et une infrastructure de base sont en place, mais l'innovation technologique et la culture de conformité intégrée restent insuffisantes. Le responsable IT résume cette situation : « Nous sommes réactifs, pas encore prédictifs ».

4. Facteurs internes et externes influençant la performance

a. Facteurs internes

Plusieurs facteurs internes influencent la performance du dispositif. Du côté positif, le leadership de la direction générale constitue un levier important. L'engagement de la DG renforce la légitimité de la conformité et facilite l'arbitrage budgétaire. De même, la collaboration entre IT et conformité est jugée constructive, favorisant une réponse rapide aux besoins.

En revanche, le sous-dimensionnement humain et l'absence d'outils analytiques avancés freinent la modernisation. L'audit interne souligne également un manque de standardisation et de formalisation dans la documentation des alertes, qui pourrait poser un problème en cas de contrôle externe.

Facteur	Influence	Commentaire
Leadership de la DG	+	Soutien stratégique visible
Collaboration IT	+	Bonne communication avec la conformité
Charge de travail	-	Sous-dimensionnement humain
Absence d'outils avancés	-	Freine la modernisation du système

b. Facteurs externes

Parmi les facteurs externes, la réglementation COBAC apparaît comme un cadre clarifié et harmonisé, offrant une base solide.

Toutefois, l'interaction avec l'ANIF reste insuffisante, privant la banque de retours utiles. Le marché local des talents est limité, ce qui restreint la capacité à recruter des profils spécialisés. Enfin, le contexte régional – forte utilisation du cash, risques de corruption, flux transfrontaliers – complexifie le filtrage et augmente le bruit dans les systèmes AML. Ces facteurs externes accentuent la difficulté d'atteindre un niveau de maturité avancé.

Facteur	Influence	Commentaire
Règlementation COBAC	+	Clarifiée et harmonisée
Interaction ANIF	-	Rétroaction insuffisante
Disponibilité des talents	-	Marché local encore restreint
Risque régional (cash, corruption)	-	Complexifie le filtrage des flux

5. Synthèse SWOT du dispositif actuel

- Forces : gouvernance active, implication de la direction, analystes certifiés, système AML interfacé.
- Faiblesses : taux élevé de faux positifs, système statique, absence d'analyse comportementale, manque de ressources spécialisées.
- Opportunités : intégration de l'IA et du machine learning, partenariats Fintech, centralisation régionale des compétences.
- Menaces : renforcement réglementaire exigeant, risque réputationnel en cas de défaillance, concurrence interbancaire sur la perception de la robustesse.

Cette matrice illustre le potentiel de progression du dispositif, à condition d'investir simultanément dans la technologie, l'organisation et le capital humain.

L'évaluation du dispositif de détection des transactions suspectes de BGFIBANK Congo met en lumière un paradoxe. La structure institutionnelle est solide : gouvernance active, outils de base opérationnels, capital humain engagé. Pourtant, l'efficacité opérationnelle est bridée par un taux excessif de faux positifs, l'absence d'outils analytiques avancés et une surcharge de travail sur des équipes limitées. Le

décalage avec les bonnes pratiques internationales se creuse, faisant apparaître un besoin urgent d'optimisation.

PARTIE III – Stratégies d'optimisation et recommandations

Chapitre 8 – Leviers technologiques

Introduction du chapitre

L'analyse des entretiens avec les responsables conformité, analystes AML, gestionnaires de clientèle, responsables IT et opérationnels a mis en lumière une réalité contrastée : BGFIBANK Congo dispose d'une infrastructure technique de base solide (AML Watch interfacé avec T24, reporting automatisé vers l'ANIF), mais cette configuration demeure rigide, statique et génère un volume excessif de faux positifs. Les équipes conformité, malgré leur engagement, expriment une fatigue opérationnelle et un manque de moyens analytiques pour aller au-delà de la simple gestion des alertes. La voie d'optimisation passe donc par un repositionnement technologique intégrant des solutions intelligentes, automatisées et adaptées aux spécificités locales.

1. Intégration de l'Intelligence Artificielle et du Machine Learning

a. Objectifs de l'IA dans le contexte LCB-FT

L'objectif premier de l'IA est de réduire le taux anormalement élevé de faux positifs (>90 % des alertes). Les analystes ont souligné que le système génère de multiples alertes répétitives pour les mêmes clients, faute d'apprentissage dynamique. L'IA doit permettre d'analyser les comportements transactionnels dans leur globalité et de distinguer les variations légitimes des signaux suspects. Elle doit également soulager les analystes, aujourd'hui submergés, en leur permettant de se concentrer sur les cas à forte valeur ajoutée. Enfin, elle constitue une réponse à l'évolution des typologies de risques (cash intensif, flux transfrontaliers, dépôts itératifs), difficiles à capturer par des scénarios statiques.

b. Algorithmes recommandés

L'approche la plus adaptée repose sur une combinaison de modèles. Les algorithmes de détection d'anomalies, tels que l'Isolation Forest ou les Autoencoders, sont pertinents pour repérer des transactions atypiques sans supervision préalable. Des techniques de clustering (DBSCAN, K-Means) permettraient de segmenter les clients selon leurs comportements transactionnels réels, réduisant les alertes injustifiées. Enfin, les réseaux de neurones supervisés pourraient être entraînés sur les cas passés validés par les analystes et l'ANIF, renforçant ainsi la pertinence des signaux. L'utilisation de modèles hybrides, croisant règles existantes et apprentissage automatique, faciliterait la transition.

c. Étapes d'implémentation pour BGFIBANK Congo

La mise en œuvre devrait se faire en plusieurs phases progressives. D'abord, une phase pilote consisterait à entraîner un modèle IA sur un échantillon historique d'alertes classées (pertinentes ou non) afin de tester la capacité prédictive. Ensuite, l'intégration hybride permettrait de conserver les scénarios actuels tout en laissant l'IA proposer des scores de risque complémentaires. Enfin, une boucle de rétroaction continue, alimentée par les analystes, permettrait d'affiner les seuils et d'améliorer la précision des modèles. Ce processus réduirait la lassitude exprimée par les analystes et améliorerait significativement l'efficience.

Architecture d'intégration proposée pour un moteur IA LCB-FT

1. Création d'un Data Lake AML (centralisation de l'historique client)
2. Nettoyage et normalisation des données (via outils ETL)
3. Développement d'un moteur IA local (avec supervision du Groupe BGFIBANK)
4. Tests en environnement bac à sable
5. Déploiement progressif sur segments prioritaires (corporate)

(Schéma : données – modèles ML – scoring – feedback analyste – ajustement)

2. Usage avancé des Graph Analytics

a. Pourquoi les graphes ?

Les interviews ont montré que les analystes peinent à relier des transactions isolées en schémas cohérents, particulièrement pour les flux transfrontaliers ou les dépôts cash répétés suivis de transferts internationaux. Or, les circuits de blanchiment et de financement du terrorisme reposent souvent sur des réseaux de comptes, d'intermédiaires et d'entités liées par des connexions indirectes. L'approche par graphes permet de cartographier ces relations et de visualiser les « hubs » suspects, là où se concentre un flux disproportionné.

b. Mise en œuvre recommandée

Étape	Action
1	Extraction des relations (client-client, compte-compte, bénéficiaire effectif)
2	Modélisation dans une base de graphes (Neo4j, GraphX)
3	Détection de motifs suspects (motifs circulaires, multi-sauts)
4	Enrichissement via des données externes (registres publics, sanctions)

c. Cas d'usage prioritaire à BGFIBANK Congo

Trois cas d'usage ressortent des entretiens. Premièrement, l'identification des réseaux transfrontaliers impliquant plusieurs comptes dispersés mais reliés à une même entité économique. Deuxièmement, l'analyse des dépôts cash atypiques suivis de transferts vers l'international, pratique fréquente dans le contexte congolais. Enfin, la détection de chaînes de paiements répétitifs vers des zones sensibles, qui échappent aux règles statiques actuelles.

3. Automatisation des processus (RPA)

a. Bénéfices clés de la RPA

Les analystes soulignent passer un temps excessif sur des tâches administratives répétitives : collecte documentaire, saisie manuelle, extraction d'alertes. La robotisation de ces tâches réduirait la surcharge immédiate et permettrait de réallouer les ressources aux enquêtes.

b. Processus prioritaires à automatiser

Processus	Avant (manuel)	Après (automatisé)	Gain estimé
Extraction des justificatifs KYC	15 min / client	3 min	80 %
Filtrage quotidien contre les listes	2h / jour	20 min	83 %
Préparation DOD (Déclaration d'Opération Douteuse)	1h / cas	15 min	75 %

c. Déploiement progressif

1. Cartographie des processus éligibles à la RPA
2. Sélection d'un outil RPA (UiPath, Blue Prism, Power Automate)
3. Développement de scripts par processus
4. Supervision des robots par la conformité (niveau 1)
5. Mesure des performances et ajustements

Exemple : Banque Centrale du Kenya a automatisé la remontée des déclarations AML par RPA en 2022 – réduction de 70 % des erreurs de transmission.

Les leviers technologiques présentés dans ce chapitre constituent une opportunité stratégique pour BGFIBANK Congo. En intégrant l'intelligence artificielle, l'analyse de graphes et la RPA, la banque pourra :

- Réduire la pression sur les analystes ;
- Améliorer la qualité des alertes ;
- Renforcer sa conformité aux standards internationaux.

Le prochain chapitre traitera des leviers organisationnels, en complément de cette approche technocentrée.

Chapitre 9 – Leviers organisationnels et humains

Introduction du chapitre

La transformation d'un dispositif LCB-FT ne repose pas uniquement sur les outils technologiques. Elle nécessite une réorganisation structurelle et fonctionnelle au sein de la banque, afin de favoriser une approche transversale, proactive et réactive de la gestion des risques. Ce chapitre met en lumière les principaux leviers organisationnels qui permettraient à BGFIBANK Congo d'optimiser son dispositif de détection et de traitement des transactions suspectes. Trois axes sont analysés : le renforcement des comités et de la gouvernance, le déploiement d'un KYC dynamique, et l'amélioration des trois lignes de défense.

1. Création de comités transversaux et collaboration renforcée

a. Limites actuelles

Les entretiens avec les responsables opérations et commerciaux ont montré que le manque de coordination est un frein majeur. Les blocages de virements SWIFT, par exemple, nuisent à la satisfaction des clients corporate.

b. Recommandations

La création d'un comité transversal réunissant conformité, opérations, commercial et IT permettrait de résoudre rapidement les cas urgents. Un canal d'escalade rapide (hotline ou messagerie sécurisée) doit compléter ce dispositif.

c. Bénéfices attendus

- Fluidité de l'information entre départements
- Réactivité accrue face à des typologies émergentes
- Décloisonnement de la fonction conformité

Figure 1 : Nouvelle gouvernance transversale recommandée

(Schéma de comité central et cellules spécialisées en étoile)

2. Profil de risque client dynamique et KYC temps réel

a. Constat

- Le KYC est réalisé à l'entrée en relation, puis rarement mis à jour ;
- Le profil de risque est figé : pas de mécanisme d'adaptation aux changements comportementaux ;
- Faible corrélation entre le KYC et le système de scoring AML ;
- Le dispositif actuel repose sur des profils statiques qui déclenchent des alertes répétitives, même lorsque les comportements évoluent de manière légitime.

b. Composantes d'un KYC dynamique

Un profil dynamique inclurait l'intégration en temps réel des données transactionnelles, des informations externes (PEP, sanctions) et des indicateurs de comportement.

Exemple : Société Générale a mis en place un KYC dynamique via API connectées à des bases publiques et privées.

c. Étapes de mise en œuvre

1. Cartographie des segments clients à fort risque
2. Mise en place d'une base de données centralisée KYC
3. Définition d'un scoring évolutif (KYC + activité)
4. Création d'un flux de mise à jour automatisé (cf. RPA – Chapitre 8)

Figure 2 : Cycle de vie d'un profil client dynamique

(Graphique avec étapes : onboarding – scoring – surveillance – révision – archivage)

3. Spécialisation des analystes conformité

a. Limites du modèle actuel

- Les analystes sont polyvalents mais surchargés, sans temps pour développer une expertise sectorielle.
- Une équipe AML généraliste, composée de 4 analystes couvrant tous types de clients (particuliers, entreprises, institutions) ;
- Traitement des alertes selon un ordre d'arrivée, sans segmentation par typologie ;
- Absence de spécialisation fonctionnelle (fraude interne, structuration, transferts internationaux).

b. Recommandations

Créer des pôles spécialisés (trade finance, cash intensif, fraude documentaire, flux transfrontaliers).

Axe de spécialisation	Objectif	Résultat attendu
Segment client	Créer des analystes experts Corporate, Retail, Public	Détection ciblée et contextualisée
Typologie de risque	Dédier des analystes à la fraude, au FT, aux PEP	Montée en expertise sectorielle
Source d'alerte	Distinguer les alertes automatiques des remontées humaines	Traitement différencié des cas

4. Mise en place de Programmes de formation certifiante

a. Diagnostic actuel

- Les formations AML à BGFIBANK Congo sont encore informelles, internes, sans certification externe ;
- Absence de trajectoire claire de développement professionnel pour les analystes ;

- Très peu d'opportunités d'échanges régionaux ou internationaux.
- Les équipes sont certifiées COBAC niveau 2, mais peu exposées aux standards internationaux.

b. Certifications recommandées

Organisme	Programme	Reconnaissance
ACAMS	Certified Anti-Money Laundering Specialist (CAMS)	Référence internationale
ICA	Diploma in AML	Fort en Afrique anglophone
COBAC	Certification régionale AML (niveau 2/3)	Reconnaissance CEMAC
FIBA	AML Compliance Certificate	Fort en zones francophones émergentes

c. Plan de formation proposé

- Phase 1 (0–6 mois) : Évaluation des compétences existantes et identification des gaps ;
- Phase 2 (6–18 mois) : Formation certifiante progressive (1 à 2 analystes tous les 6 mois) ;
- Phase 3 (18–36 mois) : Intégration d'un plan de formation continue obligatoire pour tous les acteurs LCB-FT.

Résultat attendu : montée en compétences → réduction du taux d'escalade erronée → gain de crédibilité vis-à-vis de l'ANIF.

Le renforcement du dispositif LCB-FT de BGFIBANK Congo ne peut se limiter à une transformation technologique. Il nécessite une redéfinition organisationnelle et une montée en compétence de son capital humain, impliquant :

- Une gouvernance transversale renforcée ;
- Une refonte du KYC vers un système dynamique.
- Une spécialisation des analystes conformité
- Mise en place solide de programmes de formation certifiante

Ces ajustements structurels, une fois combinés aux leviers technologiques, peuvent transformer la banque en acteur proactif, agile et résilient face aux menaces LCB-FT.

Le chapitre suivant complètera cette stratégie par les leviers humains, centrés sur la formation, la spécialisation, et la valorisation des compétences en conformité.

Chapitre 11 – Plan de mise en œuvre priorisé

Introduction du chapitre

Toute stratégie d'optimisation doit se traduire par un plan de déploiement réaliste, cohérent avec les contraintes opérationnelles de l'institution. Ce chapitre propose une feuille de route progressive pour la modernisation du dispositif de détection des transactions suspectes de BGFIBANK Congo, articulée autour de trois horizons :

- Court terme (0–12 mois) : fondations et premiers gains rapides
- Moyen terme (12–24 mois) : structuration et interconnexion
- Long terme (24–36 mois) : maturité, innovation et résilience

1. Actions court terme (0–12 mois)

a. Objectifs

- Réduction immédiate de la charge opérationnelle
- Amélioration de la qualité des alertes
- Renforcement de la gouvernance

b. Actions à lancer

Action	Responsable	Résultat attendu
Déploiement d'un robot RPA pour automatiser le prétraitement des alertes simples	IT + Conformité	Gain de temps ≥ 30 %
Révision des règles de filtrage SAP AML Watch (ajustement des seuils)	Conformité	Réduction des faux positifs
Lancement d'un Comité LCB-FT élargi avec IT, juridique, métiers	Direction Générale	Décisions opérationnelles plus transversales
Audit ciblé sur le processus DOD (frictions, délais, retour ANIF)	Audit interne	Plan d'amélioration rapide
Élaboration du référentiel de profils KYC dynamiques	Conformité + Data	Base pour le scoring comportemental

2. Actions moyen terme (12–24 mois)

a. Objectifs

- Structuration durable de la gouvernance LCB-FT

- Intégration des outils d'analyse avancée
- Spécialisation des ressources humaines

b. Actions stratégiques

Action	Responsable	Indicateur
Intégration d'un moteur d'IA (ML) dans le scoring AML (phase pilote)	IT + Conformité + Fintech partenaire	Taux de faux positifs < 70 %
Mise en œuvre du KYC dynamique connecté à l'historique client	IT + Commercial + Risques	Profils clients mis à jour automatiquement
Spécialisation des analystes par typologie de risque	DRH + Conformité	Réduction du délai moyen d'escalade
Certification ACAMS ou ICA de 2 analystes AML	DRH	50 % des analystes certifiés
Déploiement d'une base de données interconnectée (AML, KYC, risques)	IT	Plateforme unifiée de surveillance

3. Actions long terme (24–36 mois)

a. Objectifs

- Automatisation avancée
- Résilience face aux menaces émergentes
- Positionnement régional stratégique

b. Axes de transformation

Action	Responsable	Résultat attendu
Couplage IA + Graph Analytics pour la détection des réseaux de blanchiment	IT + Conformité + Groupe BGFIBANK	Capacité à cartographier les circuits criminels
Intégration du feedback ANIF dans le système AML	Direction conformité	Taux de retour sur DOD ≥ 40 %
Création d'un centre d'expertise AML régional à Brazzaville	Groupe BGFIBANK	Mutualisation des bonnes pratiques
Déploiement d'un programme de mobilité régionaledes analystes AML	DRH Groupe	Stabilité des équipes et transfert de compétences
Certification complète de l'équipe AML (ACAMS, ICA, COBAC niveau 3)	DRH	Équipe 100 % certifiée d'ici 36 mois

4. Tableau de synthèse des indicateurs de performance (KPI)

Axe	Indicateur	Cible à 36 mois
Alertes AML	Taux de faux positifs	< 65 %
Performance RH	Analystes certifiés	100 %
Efficacité	Temps moyen de traitement d'alerte	< 24h
Collaboration	Fréquence des comités transversaux	≥ 1 / mois
Profilage client	Profils dynamiques actifs	90 % du portefeuille
Outils avancés	IA + Graphes opérationnels	Oui
Réputation	Retour positif de l'ANIF / audits	≥ 2 / an

Figure 1 : Feuille de route visuelle (Gantt simplifié 0–36 mois)

(à insérer dans la version finale)

Le plan de mise en œuvre présenté dans ce chapitre offre à BGFIBANK Congo une trajectoire progressive mais ambitieuse pour faire évoluer son dispositif LCB-FT vers les standards les plus avancés, tout en tenant compte des réalités locales. Chaque phase est construite de façon modulaire, mesurable, et ajustable, pour garantir une montée en maturité durable.

Ce plan ouvre la voie à la conclusion générale de cette thèse, où seront synthétisés les apports, limites et perspectives de cette démarche d'optimisation.

Conclusion générale

Au terme de notre étude, il est temps de revenir à notre question de départ qui visait à identifier les leviers d'optimisation du dispositif de détection des transactions suspectes au sein de BGFIBANK CONGO. Notre parcours nous a d'abord menés à établir le cadre conceptuel et réglementaire complexe dans lequel la banque évolue, un environnement marqué par des menaces sophistiquées et des exigences normatives multi-niveaux, du GAFI à l'ANIF en passant par la COBAC.

L'analyse des entretiens avec les acteurs clés – analystes AML, responsables conformité, gestionnaires de clientèle, responsables des opérations, de l'audit interne, du commercial et de l'IT – a mis en évidence plusieurs constats majeurs. D'une part, la banque dispose d'un socle réglementaire et technique robuste, conforme aux prescriptions de la COBAC et de l'ANIF, notamment à travers l'utilisation d'outils comme AML Watch et l'interfaçage avec T24. D'autre part, ce socle se révèle insuffisant face aux défis spécifiques du marché congolais : forte utilisation du cash, importance des flux transfrontaliers, faiblesse de la digitalisation des PME, lenteur et rigidité des échanges avec les autorités de tutelle.

Les résultats des analyses entretiens ont souligné trois grandes limites du dispositif actuel. Premièrement, un déficit technologique marqué, caractérisé par des outils statiques générant un volume excessif de faux positifs et une absence de capacités analytiques avancées (IA, graphes). Deuxièmement, des tensions organisationnelles entre les départements commerciaux, opérationnels et conformité, accentuées par un manque de coordination et de mécanismes de communication rapides. Troisièmement, une fragilité humaine et culturelle, perceptible dans la démotivation des analystes, l'attractivité limitée du métier AML, et le rôle encore trop réactif de l'audit interne.

Face à ces constats, notre recherche a permis de répondre à notre problématique en identifiant un ensemble de neuf leviers d'optimisation concrets, articulés autour des axes technologiques, organisationnel et humain. Ces leviers, allant de l'instauration d'un "Comité des Cas Complexes" à l'intégration de l'intelligence artificielle, forment une réponse systémique aux défis observés. Les hypothèses de départ, suggérant que l'optimisation dépendait d'une meilleure collaboration et d'une intégration technologique intelligente, se trouvent ainsi largement confirmées par notre analyse.

Ce travail présente néanmoins certaines limites. En tant qu'étude de cas unique, ses conclusions sont spécifiques à BGFIBANK CONGO et ne sauraient être généralisées à l'ensemble du secteur bancaire sans une analyse comparative. De plus, l'accès à certaines données de performance chiffrées du dispositif a été, par nature, limité.

L'ouverture reste donc double : d'une part, vers un approfondissement de la coopération régionale et internationale, indispensable pour contrer des schémas de criminalité transnationale ; d'autre part, vers une réflexion académique plus large sur la manière dont les banques africaines peuvent adapter les innovations LCB-FT aux particularités locales sans tomber dans une transposition mécanique de modèles occidentaux.

Ainsi, la présente recherche apporte une contribution pratique et analytique en proposant un modèle d'optimisation réaliste et contextualisé. Elle invite à considérer la conformité non pas comme une contrainte administrative, mais comme un vecteur de résilience, de compétitivité et de crédibilité dans un environnement financier en mutation rapide.

ANNEXES

Annexe 1

Questionnaire d'entretien

Merci de prendre le temps de participer à cet entretien. Vos réponses contribueront à une meilleure compréhension des pratiques, des outils et des processus relatifs à la détection des transactions suspectes, et permettront d'identifier des opportunités d'optimisation. Toutes les informations seront traitées de manière confidentielle et utilisées à des fins académiques.

Titre du mémoire et cadre de l'entretien :

Optimisation du dispositif de détection des transactions suspectes : Étude de cas BGFIBANK Congo dans la lutte contre le blanchiment de capitaux et le financement du terrorisme (LCB-FT)

Plan d'entretien et contexte organisationnel

- Objectif général : Comprendre les pratiques, outils et processus liés à la détection des transactions suspectes, et identifier les opportunités d'optimisation.
- Contexte organisationnel : Décrire brièvement la structure de l'organisation, les principaux départements impliqués (Conformité, Risques, Opérations, IT), et les flux de données pertinents.

Consentement éclairé

- Vous confirmez que votre participation est volontaire et que vous consentez à ce que les informations partagées soient utilisées à des fins académiques et exploitées de manière confidentielle.
- Droit de retrait : Vous pouvez mettre fin à l'entretien à tout moment.

Section 1 — Contexte et perception générale

- Pouvez-vous décrire votre rôle dans l'organisation et vos responsabilités liées à la conformité / LCB-FT ?
- Quels sont, selon vous, les principaux défis actuels liés à la détection des transactions suspectes dans votre institution ?
- Quelles données ou sources utilisez-vous le plus fréquemment dans votre travail de détection ?

Section 2 — Dispositif technologique

- Comment évaluez-vous l'efficacité des outils actuels de détection (ex. SIRON AML, KYC, filtrage SWIFT) ?

- Quels sont, selon vous, leurs points forts et leurs limites (ex. faux positifs, ergonomie, pertinence des scénarios de risque) ?
- Quelles améliorations technologiques seraient prioritaires pour renforcer l'efficacité du dispositif ?

Section 3 — Processus humain et organisationnel

- Pouvez-vous décrire les étapes de traitement d'une alerte, de sa génération jusqu'à la décision finale ?
- Quelles difficultés rencontrez-vous dans la collaboration inter-départements (ex. délai de réponse des gestionnaires de clientèle) ?
- Existe-t-il des goulots d'étranglement ou des pertes de temps dans le processus ?

Section 4 — Culture et compétences

- Dans quelle mesure les collaborateurs sont-ils sensibilisés et formés à la lutte LCB-FT ?
- Quelles compétences ou formations manquent le plus aujourd'hui ?
- La culture de conformité est-elle suffisamment partagée au sein de l'organisation, ou reste-t-elle cantonnée au département conformité ?

Section 5 — Optimisation et perspectives

- Quelles mesures concrètes pourraient réduire la charge liée aux faux positifs ?
- Voyez-vous des opportunités d'utiliser l'intelligence artificielle, l'automatisation ou l'analyse de données pour renforcer la détection ?
- Quelles recommandations feriez-vous à la direction pour améliorer l'efficience et la performance du dispositif ?

Section 6 — Évaluation globale

- Sur une échelle de 1 à 10, comment évalueriez-vous la robustesse du dispositif actuel, et pourquoi ?
- Quels facteurs clés de succès garantiront la pérennité et l'efficacité du dispositif dans les 5 prochaines années ?

Annexe 2

Retranscription de l'Entretien - Responsable Conformité

Date : 09 avril 2025

Lieu : BGFIBANK Congo, Brazzaville

Intervieweur : Hélène EFOUTE NYAMSI

Interviewé : Responsable de la Conformité

Hélène EFOUTE NYAMSI : Bonjour Monsieur/Madame, merci de m'accorder cet entretien. Pour commencer, quelle est votre évaluation globale de l'efficacité du dispositif LCB-FT de la banque ?

Responsable Conformité : Bonjour. Je dirais que notre dispositif est **robuste et conforme** aux exigences de la COBAC. La direction générale nous soutient, ce qui est notre plus grande force. Nous avons un comité actif et des outils en place. Cependant, il y a un écart important entre être "conforme" et être réellement "efficient". C'est là que se situent nos défis.

Hélène EFOUTE NYAMSI : Pourriez-vous préciser ces défis ? Quel est le plus grand obstacle que vous rencontrez au quotidien ?

Responsable Conformité : Sans hésiter, le **volume de faux positifs**. Notre outil, SAP AML Watch, est puissant mais il fonctionne sur des règles statiques. Le résultat, c'est qu'il génère plus de 1200 alertes par mois, et nos statistiques internes montrent que plus de 90% d'entre elles, après analyse, ne sont pas pertinentes. Mes analystes, qui sont très compétents, passent une part énorme de leur temps à écarter du "bruit". C'est notre principal goulot d'étranglement.

Hélène EFOUTE NYAMSI : Comment cette surcharge impacte-t-elle le travail de vos équipes ?

Responsable Conformité : L'impact est double. D'abord, une **charge de travail immense**. J'ai quatre analystes qui traitent chacun une soixantaine d'alertes par jour. C'est intenable sur le long terme et cela augmente le risque de lassitude, voire d'erreur. Ensuite, cela nous empêche de développer une **véritable spécialisation**. Aujourd'hui, tout le monde traite de tout. Idéalement, j'aimerais avoir un expert sur la fraude documentaire, un autre sur les flux liés au commerce international, etc. Nous n'avons pas le temps pour cette montée en expertise.

Hélène EFOUTE NYAMSI : Lorsque le doute sur une alerte persiste, vous sollicitez les gestionnaires de clientèle. Comment se passe cette collaboration ?

Responsable Conformité : C'est le second grand défi : les **silos**. La collaboration est professionnelle, mais pas toujours fluide. Le gestionnaire commercial a ses propres objectifs, et nos demandes de justificatifs sont parfois vues comme une contrainte administrative qui ralentit le business. Obtenir une réponse rapide et complète peut prendre plusieurs jours, ce qui retarde toute la chaîne d'investigation.

Hélène EFOUTE NYAMSI : Et une fois que vous transmettez une Déclaration d'Opération Douteuse à l'ANIF, quel est le suivi ?

Responsable Conformité : C'est un point sensible. La **rétroaction de l'ANIF est quasi inexistante**. Nous envoyons nos rapports, mais nous ne savons que très rarement si cela a abouti à une enquête ou à une action en justice. Ce manque de retour est un peu démotivant pour les équipes, qui ont parfois l'impression de travailler dans le vide.

Hélène EFOUTE NYAMSI : Pour conclure, si vous aviez un levier d'optimisation prioritaire à activer, quel serait-il ?

Responsable Conformité : La technologie, sans aucun doute. Il nous faut des outils plus intelligents. L'intégration de **l'intelligence artificielle** ou du **machine learning** pour analyser les comportements et non plus seulement des règles fixes. Cela permettrait de mieux cibler les vrais risques, de réduire les faux positifs et de libérer mes analystes pour qu'ils se concentrent sur des enquêtes à forte valeur ajoutée. Nous devons passer d'une conformité réactive à une gestion des risques proactive.

Annexe 3

Retranscription de l'Entretien - Responsable de l'Audit Interne

Date : 16 mai 2025

Lieu : BGFIBANK Congo, Brazzaville

Intervieweur : Hélène EFOUTE NYAMSI

Interviewé : Responsable de l'Audit Interne (anonymisé)

Hélène EFOUTE NYAMSI : (Section 1) Bonjour. En tant que Responsable de l'Audit, comment situez-vous le risque LCB-FT dans la cartographie des risques de la banque ?

Responsable de l'Audit Interne : Bonjour. Le risque LCB-FT est classé comme un **risque majeur et transversal**. Il impacte directement notre risque de non-conformité, notre risque opérationnel et, surtout, notre risque réputationnel. Notre rôle, en tant que troisième ligne, est de fournir une assurance indépendante sur l'adéquation et l'efficacité du dispositif mis en place par les première et deuxième lignes de défense pour maîtriser ce risque.

Hélène EFOUTE NYAMSI : (Section 2) Lors de vos missions, quelle est votre évaluation des outils technologiques de détection ?

Responsable de l'Audit Interne : Nos audits confirment que les outils en place sont fonctionnels et permettent de répondre aux exigences réglementaires de base. La piste d'audit au sein du système est traçable, ce qui est un point essentiel pour nous. Cependant, nous avons relevé dans nos rapports que l'efficacité du système est **fortement dépendante du paramétrage des scénarios**. Un paramétrage qui n'est pas régulièrement revu et affiné peut conduire soit à une surcharge d'alertes non pertinentes, soit, plus grave, à ne pas détecter de nouvelles typologies de fraude.

Hélène EFOUTE NYAMSI : (Section 3) Le processus humain de traitement des alertes, tel qu'il est documenté, est-il bien respecté en pratique ?

Responsable de l'Audit Interne : Dans l'ensemble, la procédure est suivie. Le principe de validation par un supérieur hiérarchique est respecté, ce qui est un point de contrôle fort. Néanmoins, nos tests d'audit ont parfois mis en évidence des **délais de traitement hétérogènes**, notamment dans la phase de collecte d'informations auprès des métiers. Nous avons également recommandé une plus grande standardisation dans la documentation des décisions de clôture d'alerte, afin de garantir une piste d'audit irréprochable en cas de contrôle externe.

Hélène EFOUTE NYAMSI : (Section 4) Quelle est votre perception de la culture de conformité au sein de l'organisation ?

Responsable de l'Audit Interne : Le "ton au sommet" est bon ; l'implication de la Direction est claire. Le principal axe d'amélioration, commun à beaucoup de banques, est la diffusion de cette culture jusqu'à la première ligne de défense. Nos missions montrent que la perception du risque LCB-FT est encore parfois vue comme l'unique responsabilité du département Conformité. Le renforcement de la **responsabilisation des gestionnaires de clientèle** sur la qualité du KYC et la remontée d'informations est un point que nous suivons attentivement.

Hélène EFOUTE NYAMSI : (Section 5) Quelles recommandations feriez-vous pour améliorer la performance du dispositif ?

Responsable de l'Audit Interne : D'un point de vue de l'audit, toute optimisation doit être maîtrisée et contrôlable. L'introduction de l'IA, par exemple, est une piste intéressante à condition de définir un cadre de gouvernance très strict pour que les modèles ne deviennent pas des "boîtes noires". Ma recommandation principale serait de **renforcer la formalisation et la mesure de la performance** : des indicateurs de performance (KPIs) clairs sur la qualité et les délais de traitement, et une meilleure traçabilité des échanges entre la Conformité et les métiers.

Hélène EFOUTE NYAMSI : (Section 6) Sur 10, comment évalueriez-vous la "maîtrise" du dispositif actuel ?

Responsable de l'Audit Interne : Je lui attribuerais un **7/10**. Le dispositif est **conforme** aux exigences, et les contrôles fondamentaux existent. Il n'y a pas de faiblesse majeure critique. Cependant, il n'est pas encore **optimisé**. Il y a des zones d'inefficience qui, à terme, peuvent devenir des risques. Les facteurs clés de succès pour l'avenir sont la qualité des données, une collaboration inter-départementale formalisée, et la capacité à faire évoluer la technologie dans un cadre de contrôle parfaitement maîtrisé.

Annexe 4

Retranscription de l'Entretien - Gestionnaire de Clientèle

Date : 09 mai 2025

Lieu : BGFIBANK Congo, Brazzaville

Intervieweur : Hélène EFOUTE NYAMSI

Interviewé : Gestionnaire de Clientèle (anonymisé)

Hélène EFOUTE NYAMSI : Bonjour, merci pour votre temps. En tant que gestionnaire de clientèle, comment décririez-vous votre rôle dans le dispositif LCB-FT ?

Gestionnaire de Clientèle : Bonjour. Notre rôle est double. D'abord, nous sommes responsables de la connaissance de nos clients, le fameux KYC, à l'entrée en relation. Ensuite, nous sommes le point de contact lorsque la Conformité a des questions. Notre mission première reste le développement commercial, mais la conformité est une partie intégrante de la gestion du risque de notre portefeuille.

Hélène EFOUTE NYAMSI : Concrètement, que se passe-t-il lorsque la Conformité vous contacte pour une alerte sur un de vos clients ?

Gestionnaire de Clientèle : Je reçois une demande par courriel, souvent assez technique, me demandant de justifier une ou plusieurs opérations. Mon travail consiste alors à contacter mon client pour obtenir des explications ou des documents, comme une facture ou un contrat.

Hélène EFOUTE NYAMSI : Quelles sont les principales difficultés que vous rencontrez dans ce processus ?

Gestionnaire de Clientèle : La principale difficulté est de **maintenir une relation de confiance avec le client**. Poser des questions qui peuvent paraître inquisitrices sur l'origine ou la destination de ses fonds est un exercice très délicat. Il faut être diplomate pour ne pas le froisser. Le deuxième défi est **le temps**. Je suis souvent à l'extérieur. Le temps de joindre le client, d'obtenir les bons documents et de formaliser une réponse peut prendre un ou deux jours. Pendant ce temps, je sais que la Conformité attend et qu'ils ont leurs propres délais à respecter. On se sent parfois pris entre deux feux : les exigences internes et la satisfaction du client.

Hélène EFOUTE NYAMSI : Comment décririez-vous la collaboration avec le département Conformité ?

Gestionnaire de Clientèle : Elle est professionnelle. Nous comprenons leur rôle, mais nous n'avons pas toujours toutes les clés pour comprendre le "pourquoi" de leurs demandes. Parfois, une opération qui nous semble parfaitement logique d'un point de vue commercial va déclencher une alerte. On a le sentiment qu'un dialogue plus en amont nous aiderait à mieux anticiper leurs attentes.

Hélène EFOUTE NYAMSI : Selon vous, qu'est-ce qui pourrait améliorer cette collaboration ?

Gestionnaire de Clientèle : Des échanges plus réguliers, peut-être. Une sorte de **comité ou de réunion rapide sur les cas complexes**, où l'on pourrait discuter du contexte "business" d'un dossier. Cela permettrait de lever des doutes plus vite et de travailler plus en partenariat. On serait plus dans la "gestion commune du risque" que dans un simple échange de questions-réponses.

Annexe 5

Retranscription de l'Entretien - Responsable Conformité 2

Hélène EFOUTE NYAMSI : (Section 1) Pourriez-vous décrire votre rôle et les principaux défis actuels liés à la détection ?

Responsable Conformité : Mon rôle est de piloter la stratégie LCB-FT, de superviser les opérations de détection et d'assurer le reporting au Comité des Risques et à la Direction Générale. Le défi principal est sans conteste l'efficience. Nous sommes conformes, mais nous le sommes au prix d'un effort immense à cause du volume de "faux positifs" que nos systèmes génèrent. Notre enjeu est de passer d'une conformité subie à une gestion du risque intelligente.

Hélène EFOUTE NYAMSI : (Section 2) Comment évaluez-vous l'efficacité des outils actuels comme SIRON AML ?

Responsable Conformité : Ils sont robustes et font le travail de base : le filtrage, la surveillance sur la base de règles. C'est leur force. Leur limite, cependant, est qu'ils sont statiques. Ils n'ont pas de capacité d'apprentissage ou d'analyse comportementale. Un client dont l'activité évolue légitimement peut générer des alertes tous les mois. L'amélioration prioritaire serait donc d'intégrer une couche d'intelligence artificielle pour mieux contextualiser les alertes et en réduire le bruit.

Hélène EFOUTE NYAMSI : (Section 3) Pouvez-vous décrire le processus de traitement d'une alerte et les difficultés de collaboration que vous rencontrez ?

Responsable Conformité : Le processus est structuré : l'alerte est assignée, un analyste fait une première analyse de "levée de doute". Si le doute persiste, il doit solliciter le gestionnaire de clientèle. C'est notre principal goulot d'étranglement. La collaboration est bonne mais les délais de réponse des métiers peuvent être longs, ce qui retarde toute la chaîne. Ils ont des priorités commerciales, nous avons des délais réglementaires. C'est une tension structurelle.

Hélène EFOUTE NYAMSI : (Section 4) La culture de conformité est-elle suffisamment partagée selon vous ?

Responsable Conformité : Elle progresse, notamment grâce au soutien visible de la direction. Cependant, elle reste encore trop cantonnée à notre département. La première ligne de défense, les métiers, a encore besoin d'être renforcée. En termes de compétences, il nous manque une spécialisation plus poussée au sein de l'équipe (sur les nouvelles typologies, la data science...) et des parcours de formation certifiants pour valoriser nos experts.

Hélène EFOUTE NYAMSI : (Section 5) Quelles recommandations feriez-vous à la direction pour améliorer l'efficience ?

Responsable Conformité : Ma recommandation se décline en trois axes, comme dans votre étude. **Technologique :** investir dans l'IA pour réduire les faux positifs. **Organisationnel :** créer des comités transversaux pour casser les silos et rendre le KYC plus dynamique. **Humain :** investir dans la formation certifiante et créer un vrai parcours de carrière pour les métiers de la conformité, afin de retenir nos talents.

Hélène EFOUTE NYAMSI : (Section 6) Sur une échelle de 1 à 10, comment évalueriez-vous la robustesse du dispositif actuel ?

Responsable Conformité : Je lui mettrais un **6,5/10**. Pourquoi ? Parce que les fondations sont solides : la gouvernance est là, nous avons des outils et une équipe dédiée. Mais nous sommes en retard sur l'efficience et l'innovation technologique, ce qui nous rend vulnérables et nous coûte cher en temps humain. Le facteur clé de succès pour les 5 prochaines années sera notre capacité à intégrer l'intelligence dans nos processus, et à faire de la conformité l'affaire de tous, pas seulement de quelques experts.

Annexe 6

Retranscription de l'Entretien - Responsable des Opérations

Date : 12 mai 2025

Lieu : BGFIBANK Congo, Brazzaville

Intervieweur : Hélène EFOUTE NYAMSI

Interviewé : Responsable des Opérations (anonymisé)

Hélène EFOUTE NYAMSI : Bonjour Monsieur/Madame, merci pour votre temps. Pouvez-vous nous décrire l'interaction entre votre Direction et celle de la Conformité concernant la LCB-FT ?

Responsable des Opérations : Bonjour. Notre interaction est principalement opérationnelle et souvent réactive. Elle se cristallise autour des blocages de transactions. Quand un paiement, typiquement un virement international, est stoppé par le filtre de sanctions (SWIFT Sanction Screening), il apparaît dans nos systèmes comme étant "en suspens". C'est à ce moment que nous entrons en communication avec la Conformité.

Hélène EFOUTE NYAMSI : Quel est le processus exact lorsqu'une transaction est bloquée ?

Responsable des Opérations : Le processus est simple : l'opération est mise en attente et n'est pas exécutée. La Conformité reçoit une alerte qu'elle doit analyser. Notre rôle est alors d'attendre leur instruction : soit la levée du blocage pour que nous puissions traiter l'opération, soit le rejet définitif. Pendant ce temps, le client attend et le flux de traitement est interrompu.

Hélène EFOUTE NYAMSI : Quels sont les principaux défis que cela pose à votre département au quotidien ?

Responsable des Opérations : Le défi numéro un est le **délai**. Une analyse peut prendre de quelques minutes à plusieurs heures. Pour une opération urgente d'un client ‘‘corporate’’, ce délai peut avoir des conséquences commerciales importantes. Nous sommes en première ligne pour gérer l'insatisfaction du client, sans toujours avoir de visibilité sur le temps que prendra la résolution. Le second défi est celui des **faux positifs de filtrage**, lorsqu'une transaction est bloquée pour une simple homonymie. C'est fréquent et cela génère des interruptions pour des opérations parfaitement légitimes.

Hélène EFOUTE NYAMSI : De votre point de vue, comment pourrait-on fluidifier cette collaboration ?

Responsable des Opérations : La communication est clé. Un **processus d'escalade clair** pour les cas urgents, avec un canal de discussion plus direct entre l'analyste Conformité et l'opérateur, pourrait accélérer les choses. Parfois, un simple contexte que nous pouvons fournir sur le client ou l'opération permettrait de lever le doute en quelques minutes. Plus de **transversalité** dans le traitement des cas complexes serait bénéfique pour tout le monde : la Conformité, les Opérations, et au final, le client.

Annexe 7

Retranscription de l'Entretien - Analyste LCB-FT

Date : [Date de l'entretien]

Lieu : BGFIBANK Congo, Brazzaville

Intervieweur : Hélène EFOUTE NYAMSI

Interviewé : Analyste LCB-FT (anonymisé)

Hélène EFOUTE NYAMSI : Bonjour, merci de prendre le temps pour cet échange. Pourriez-vous me décrire votre journée type ?

Analyste LCB-FT : Bonjour. Ma journée est rythmée par la file d'attente des alertes générées par le système. On arrive le matin, il y en a déjà des dizaines. L'objectif est de traiter son portefeuille d'alertes, ce qui représente entre 50 et 70 cas par jour. C'est un travail de volume, très intense.

Hélène EFOUTE NYAMSI : Sur ce volume, quelle est la proportion d'alertes qui débouche sur une réelle suspicion ?

Analyste LCB-FT : Très, très faible. C'est le cœur de notre problème au quotidien. La grande majorité, je dirais **plus de 90%, sont des faux positifs**. On passe un temps considérable à justifier et documenter des opérations tout à fait normales pour nos clients. Le système n'est pas dynamique ; il ne semble pas apprendre des alertes que nous avons déjà clôturées par le passé. C'est frustrant de traiter la même alerte pour le même client tous les mois.

Hélène EFOUTE NYAMSI : Et quand une alerte nécessite plus d'informations, comment se passe la communication avec les gestionnaires de clientèle ?

Analyste LCB-FT : C'est souvent là que ça ralentit. Il faut envoyer un courriel, attendre une réponse, parfois relancer. Les gestionnaires sont concentrés sur leurs objectifs commerciaux, ce que je comprends, mais nous, nous avons des délais réglementaires à tenir. On sent bien qu'on est parfois perçu comme un frein. Obtenir un simple justificatif peut parfois prendre un ou deux jours, ce qui bloque l'avancement de nos dossiers.

Hélène EFOUTE NYAMSI : Vous sentez-vous suffisamment formé pour aborder tous les types de dossiers ?

Analyste LCB-FT : La formation de base est bonne, mais nous sommes des généralistes. Quand on fait face à un montage très complexe avec des sociétés-écrans ou des flux liés à des zones géographiques inhabituelles, on manque parfois d'une expertise pointue. Une **spécialisation** par type de risque serait un vrai plus pour aller plus vite et plus loin dans l'analyse.

Hélène EFOUTE NYAMSI : Et après avoir transmis une Déclaration d'Opération Douteuse (DOD), quel est le suivi ?

Analyste LCB-FT : C'est une boîte noire. On fait notre travail d'enquête, on rédige le rapport, on le transmet... et c'est tout. On n'a **jamais de retour de l'ANIF** pour nous dire si notre dossier a été utile ou a mené à quelque chose. C'est dommage, car un feedback, même simple, donnerait plus de sens à notre travail.

Hélène EFOUTE NYAMSI : Si vous pouviez changer une seule chose, quelle serait-elle ?

Analyste LCB-FT : La **qualité des alertes**. Avoir un système plus intelligent qui nous donnerait moins de "bruit" et plus de cas réellement suspects à investiguer. On passerait moins de temps à faire de l'administratif et plus de temps à faire notre vrai métier : l'enquête.

Annexe 9

Retranscription de l'Entretien - Manager Commercial

Date : 20 mai 2025

Lieu : BGFIBANK Congo, Brazzaville

Intervieweur : Hélène EFOUTE NYAMSI

Interviewé : Manager Commercial (anonymisé)

Hélène EFOUTE NYAMSI : (Section 1) Bonjour. En tant que manager commercial, comment intégrez-vous les exigences LCB-FT dans le pilotage de votre équipe ?

Manager Commercial : Bonjour. Mon rôle est de m'assurer que nous atteignons nos objectifs de performance commerciale, mais en respectant scrupuleusement le cadre de risque de la banque. La LCB-FT est une contrainte forte mais non négociable. Le principal défi pour mon équipe est d'intégrer cette vigilance dans le geste commercial au quotidien, sans que cela ne nuise à la fluidité de la relation client et à notre efficacité. C'est un exercice d'équilibre permanent.

Hélène EFOUTE NYAMSI : (Section 3) Quelle est votre perception du processus de traitement des alertes et de la collaboration avec la Conformité ?

Manager Commercial : Le processus est souvent perçu comme une "boîte noire" par mes collaborateurs. Un gestionnaire de clientèle peut se voir bloqué sur un dossier pendant plusieurs jours en attendant un retour de la Conformité, ou en essayant d'obtenir un justificatif d'un client. Cela impacte directement son temps et sa performance. La collaboration est professionnelle, mais on gagnerait à avoir plus de dialogue en amont pour que mes équipes comprennent mieux les attentes et que la Conformité, de son côté, comprenne mieux la réalité économique de nos clients.

Hélène EFOUTE NYAMSI : (Section 4) Comment la culture de conformité est-elle vécue par la "première ligne de défense" que vous représentez ?

Manager Commercial : C'est un axe de progrès. La formation annuelle est suivie, mais elle reste souvent théorique. Le message de la direction est clair, mais sa traduction en objectifs concrets pour un commercial l'est moins. L'indicateur de performance principal reste le volume d'affaires. Intégrer un **indicateur de performance (KPI) lié à la qualité des dossiers KYC** ou à la pertinence des informations transmises, par exemple, serait un signal fort pour montrer que la conformité est l'affaire de tous et pas seulement d'un département.

Hélène EFOUTE NYAMSI : (Section 5) Quelles améliorations pourraient, selon vous, rendre le dispositif plus efficace sans pénaliser l'activité commerciale ?

Manager Commercial : Plus de **prévisibilité** et de **transparence**. Un système de **KYC dynamique**, qui nous alerterait en amont sur un changement de profil de risque d'un client, serait une avancée majeure. Cela nous permettrait d'anticiper les questions de la Conformité plutôt que de les subir. Et bien sûr, des outils qui génèrent moins de fausses alertes sur nos bons clients nous feraient gagner un temps collectif précieux.

Annexe 10

Retranscription de l'Entretien - Responsable IT / Data

Date : 15 mai 2025

Lieu : BGFIBANK Congo, Brazzaville

Intervieweur : Hélène EFOUTE NYAMSI

Interviewé : Responsable IT / Data (anonymisé)

Hélène EFOUTE NYAMSI : (Section 1) Bonjour. Pouvez-vous décrire votre rôle par rapport au dispositif LCB-FT et les défis que vous percevez de votre point de vue ?

Responsable IT / Data : Bonjour. Mon rôle, et celui de mon équipe, est de garantir que les plateformes technologiques supportant la LCB-FT sont opérationnelles, sécurisées et performantes. Nous gérons l'outil SAP AML Watch, son interfaçage avec le système bancaire central T24, et nous assurons l'intégrité des flux de données qui l'alimentent. Le principal défi est technique : le système actuel est basé sur une logique de règles statiques. Il est robuste, mais peu agile. Le faire évoluer pour répondre aux besoins d'analyse plus dynamiques de la Conformité est un enjeu constant.

Hélène EFOUTE NYAMSI : (Section 2) Comment évaluez-vous l'efficacité des outils actuels ? Quelles sont leurs limites et quelles améliorations seraient prioritaires ?

Responsable IT / Data : L'efficacité est correcte pour la conformité "réglementaire". L'outil filtre bien les listes de sanctions et applique les scénarios qu'on lui donne. C'est son point fort. Sa limite fondamentale est son manque d'intelligence. Il ne fait pas d'analyse comportementale avancée, il n'apprend pas des alertes passées. C'est ce qui explique le taux de faux positifs très élevé. Pour nous, l'amélioration prioritaire n'est pas de changer l'outil, mais de construire une couche d'intelligence par-dessus, via un moteur de Machine Learning qui pourrait scorer les alertes avant de les présenter aux analystes.

Hélène EFOUTE NYAMSI : (Section 3) D'un point de vue des processus et des flux de données, où se situent les principaux goulots d'étranglement ?

Responsable IT / Data : Le goulot d'étranglement principal n'est pas la vitesse de traitement, mais la qualité des données en amont. L'efficacité de l'outil AML est directement dépendante de la richesse et de l'actualisation des données KYC. Or, le profil client est souvent statique. Il y a un manque d'interconnexion dynamique entre les informations recueillies par les commerciaux et celles exploitées par le moteur de détection. Améliorer ce flux de données continu est un prérequis pour toute optimisation.

Hélène EFOUTE NYAMSI : (Section 4) Les équipes Conformité et IT collaborent-elles suffisamment sur ces sujets ?

Responsable IT / Data : Oui, la collaboration est bonne sur le plan opérationnel. Nous intervenons pour la maintenance et les nouveaux paramétrages. Cependant, nous pourrions être impliqués plus en amont, de manière plus stratégique. La Conformité exprime un besoin, et nous apportons une solution technique. Idéalement, nous devrions être ensemble à la table pour réfléchir aux futures innovations, comme dans le cadre du projet pilote de "Risk Scoring KYC" avec la Fintech française.

Hélène EFOUTE NYAMSI : (Section 5) Voyez-vous des opportunités réalistes d'utiliser l'IA ou l'automatisation pour renforcer la détection ?

Responsable IT / Data : Absolument, et c'est l'avenir. Je vois une feuille de route en trois temps.

- À court terme, la **RPA (Automatisation)** est une opportunité simple pour automatiser la collecte de données et soulager les analystes.
- À moyen terme, l'**IA/Machine Learning** est le projet clé pour réduire les faux positifs, mais cela demande de d'abord structurer nos données.
- À long terme, l'**analyse de graphes** est la solution la plus puissante pour les réseaux criminels, mais elle exige une maturité technique et des données très bien connectées. C'est tout à fait faisable de manière phasée.

Hélène EFOUTE NYAMSI : (Section 6) Sur une échelle de 1 à 10, comment évalueriez-vous la robustesse *technologique* du dispositif actuel ?

Responsable IT / Data : Je lui donnerais un **6/10**. Les fondations sont stables et sécurisées. Mais nous avons une "dette technologique" en matière d'intelligence et de proactivité. Nous sommes réactifs, pas encore prédictifs. Le facteur clé de succès pour les 5 prochaines années sera notre capacité à construire une architecture de données moderne qui permettra de déployer ces outils d'IA et d'analyse avancée.

Annexe 2 – Schémas techniques du dispositif AML de BGFIBANK Congo

Schéma 1 : Architecture simplifiée du système AML

plaintext

CopierModifier

[T24 Core Banking System]

↓

[Interface ETL]

↓

[SAP AML Watch]

↙ ↘

[Filtrage listes] [Scoring règles]

↓

[Génération d'alertes]

↓

[Analyse manuelle] → [Rapport DOD]

↓

[Transmission ANIF (Portail sécurisé)]

Schéma 2 : Cycle de traitement d'une alerte

plaintext

CopierModifier

[Détection (automatique ou manuelle)]

↓

[Analyse par analyste AML]

↓

[Escalade au CCO si doute]

↓

[Réunion Comité LCB-FT]

↓

[DOD transmise ou classée]

↓

[Archivage & Feedback]

Annexe 3 – Données statistiques internes (extrait)

Indicateur	Valeur 2024
Nombre moyen d'alertes/mois	1 260

Indicateur	Valeur 2024
Faux positifs estimés	91 %
Nombre de DOD transmises à l'ANIF	518
Temps moyen de traitement d'une alerte	2,1 jours
Nombre d'analystes AML	4
Alertes/jour/analyste	55 à 65
Alertes issues du front office	4,7 %
Alertes issues du système automatisé	95,3 %

Annexe 4 – Tableau comparatif des certifications AML

Certification	Organisme	Durée	Cible	Coût moyen
CAMS	ACAMS	4-6 mois	Analystes confirmés	1 500 USD
ICA Diploma	ICA	6-9 mois	Managers	2 200 USD
COBAC Niveau 2	COBAC	3 mois	Région CEMAC	750 USD
FIBA AML Certificate	FIBA	2 mois	Francophones	650 USD

GLOSSAIRE DES TERMES

Terme	Définition
AML (Anti-Money Laundering)	Ensemble des processus, lois et outils visant à lutter contre le blanchiment d'argent.
LCB-FT	Lutte contre le blanchiment de capitaux et le financement du terrorisme.
DOD (Déclaration d'Opération Douteuse)	Rapport transmis à l'autorité nationale (ANIF) lorsqu'une transaction suspecte est identifiée.
KYC (Know Your Customer)	Processus de vérification de l'identité et du profil d'un client bancaire.
PEP (Personne Politiquement Exposée)	Personnalité publique présentant un risque accru en matière de corruption.
SAP AML Watch	Outil de surveillance des transactions utilisé par BGFIBANK Congo pour détecter les flux suspects.
Graph Analytics	Méthode d'analyse des relations entre entités (clients, comptes, entreprises) pour détecter des schémas complexes.
RPA (Robotic Process Automation)	Automatisation de tâches répétitives via des robots logiciels.
IA (Intelligence Artificielle)	Capacité d'un système informatique à apprendre et à améliorer ses performances dans la détection d'anomalies.
False Positive	Alerte AML déclenchée à tort sur une opération légitime.
COBAC	Commission bancaire de l'Afrique centrale, régulateur des banques dans la zone CEMAC.
ANIF	Agence nationale d'investigation financière (Congo), autorité en charge de la réception et de l'analyse des DOD.
3 lignes de défense	Modèle de gouvernance où le contrôle s'exerce à 3 niveaux : métiers, conformité, audit.

Références bibliographiques (Style APA 7)

Références générales et institutionnelles

- FATF. (2022). Best Practices on Beneficial Ownership for Legal Persons. Financial Action Task Force. https://www.fatf-gafi.org
- FATF. (2023). Technology-driven Solutions in AML/CFT. https://www.fatf-gafi.org
- United Nations Office on Drugs and Crime. (2022). Global Report on Money Laundering Risks and Trends. https://www.unodc.org
- COBAC. (2023). Règlement N°01/2022/CEMAC/UMAC/COBAC relatif à la lutte contre le blanchiment de capitaux et le financement du terrorisme.
- BCEAO. (2022). Manuel de contrôle interne et conformité bancaire en Afrique de l'Ouest.

Références sur les outils technologiques et innovations AML

- Deloitte. (2022). AML Innovation in Sub-Saharan Banking : Pathways to Resilience. Deloitte Africa.
- UiPath. (2023). RPA in Financial Services : Compliance Automation Case Studies. https://www.uipath.com
- Neo4j. (2023). Graph Analytics for Financial Crime. https://neo4j.com
- ING Group. (2022). AI in AML Use Case Report. Amsterdam.
- SAP. (2022). SAP AML Watch Configuration & Reporting Manual. SAP SE.

Références sur la gouvernance, les structures organisationnelles et les lignes de défense

- Deloitte. (2023). Three Lines of Defense : Revisiting the Model in AML Context. Deloitte Risk Advisory.
- BNP Paribas. (2023). Internal Compliance Talent Strategy: Case Study AML Career Path. Paris.
- Société Générale. (2023). Rapport annuel de conformité & sécurité financière. Paris.
- Barclays Bank. (2022). Internal Audit Framework for AML Monitoring. London.
- Ecobank Nigeria. (2023). Compliance Culture Enhancement Report. Lagos.

Références sur la formation, les certifications et le développement humain

- ACAMS. (2023). Global AML Certification Trends and Curriculum. https://www.acams.org

- ICA. (2022). Compliance Career Pathways and Competency Frameworks. International Compliance Association.
- COBAC. (2023). Programme régional de certification en LCB-FT. Yaoundé.
- FIBA. (2022). Building Compliance Talent in Francophone Africa. Florida International Bankers Association.
- World Bank. (2021). Human Capital Development in Financial Compliance in Africa. Washington, D.C.

Références spécifiques à BGFIBANK et à la zone CEMAC

- BGFIBANK Groupe. (2024). Stratégie digitale et conformité 2025–2028. Document interne non publié.
- ANIF Congo. (2023). Rapport annuel sur les déclarations d'opérations suspectes 2022–2023. Brazzaville.
- CEMAC. (2022). Directive sur les obligations de vigilance à l'égard de la clientèle bancaire. Commission Bancaire.
- PwC. (2023). Conformité réglementaire bancaire dans la zone CEMAC : état des lieux et perspectives. Paris.
- KPMG. (2022). AML Risk Assessment Frameworks in Central African Banks. Johannesburg.

Références complémentaires (études, ouvrages, travaux académiques)

Abrahamyan, L. (2023). Major international competition funding and money laundering risks. *European Journal of Sport Sciences*, *2*(5), 20. https://doi.org/10.24018/ejsport.2023.2.5.86

Akinteye, S. A., Mokube, M., Ochei, D., & Vutumu, A. (2023). The impact of internal audit on improving anti-money laundering (aml) and counter terrorist financing (ctf) controls in nigeria. *UMYU Journal of Accounting and Finance Research*, *5*(1), 12–27. https://doi.org/10.61143/umyu-jafr.5(1)2023.002

Arim, A., & Wamema, J. (2022). Towards an improved framework for e-risk management for digital financial services (dfs) in ugandan banks: A case of bank of africa (uganda) limited. *JIOS*, *46*(1), 103–127. https://doi.org/10.31341/jios.46.1.6

Efuntade, A. O., & Efuntade, O. O. (2023). Internet payment system, forensic accounting and forensic investigation: 3m theory in the financial frauds. *Journal of Accounting and Financial Management*, *9*(7), 115. https://doi.org/10.56201/jafm.v9.no7.2023.pg115.130

Eijkman, Q. (2013). Digital security governance and accountability in europe: Ethical dilemmas in terrorism risk management. *Journal of Politics and Law*, *6*(4), 35. https://doi.org/10.5539/jpl.v6n4p35

Fu, Y., Chen, H., & Xiang, T. (2024). An analysis of the distinction between the crime of illegal lending and the crime of irregular issuance of financial bills in chinese judicial practice. *Science of Law Journal*, *3*(3), 193. https://doi.org/10.23977/law.2024.030325

Godefroy, T., Lascoumes, P., & Favarel-Garrigues, G. (2011). Reluctant partners?: Banks in the fight against money laundering and terrorism financing in france. *Security Dialogue*, *42*(2), 179–196. https://doi.org/10.1177/0967010611399615

Helgesson, K. S., & Mörth, U. (2018). Client privilege, compliance and the rule of law: Swedish lawyers and money laundering prevention. *Crime Law Soc Change*, *69*(3), 227–248. https://doi.org/10.1007/s10611-017-9753-8

Ji, M. (2023, 49). Big data analytics for anti -money laundering compliance in the banking industry.

Kannan, R., Reddiar, Y., Ramakrishnan, K., Eastaff, M. S., & Ramesh, S. (2022). Job characteristics of a malaysian bank's anti-money laundering system and its employees' job satisfaction.

F1000Research, *10*(1052), 17. https://doi.org/10.12688/f1000research.73234.2v2

Kozlova, V., Bezuhla, A., & Shuliak, K. (2023). Organization of activities of the state financial monitoring service of ukraine in the system of economic control. , (3). https://doi.org/10.32782/25202200/2023-3-14

Landry, K. B. H., Henri, G. N., & Fang, C. X. (2024). The impact of credit risk management on commercial banks performance in democratic republic of the congo. *International Journal of Business and Management Review*, *12*(5), 1–20. https://doi.org/10.37745/ijbmr.2013/vol12n5120

LAPTEş, R. (2023). Anti -money laundering i n the romanian banking system. *Bulletin of the Transilvania University of Braşov Series V: Economic Sciences*, *16(65)*(2), 11. https://doi.org/10. 31926/but.es.2023.16.65.2.11

McConnell, P. (2020). Danske bank—a smorgasbord of risks. *J. Bus. Account. Financ. Perspect.*, *2*(3), 17. https://doi.org/10.35995/jbafp2030017

Palakurti, N. R. (2023). Behavioral insights in banking: Managing credit risk and enhancing fraud control mechanisms. *International Journal of Advanced Research in Science, Communication and Technology*, *3*(1), 738. https://doi.org/10.48175/IJARSCT-8347U

Paul, E. O., Callistus, O., Somtobe, O., Esther, T., Somto, K. .-., Clement, O., & Ejimofor, I. (2023). Cybersecurity strategies for safeguarding customer's data and preventing financial fraud in the united states financial sectors. *International Journal on Soft Computing (IJSC)*, *14*(3), 1.

https://doi.org/10.5121/ijsc.2023.14301

Quintel, T. (2022). Data protection rules applicable to financial intelligence units: Still no clarity insight. *ERA Forum*, *23*, 53–74. https://doi.org/10.1007/s12027-021-00697-z

Ryder, N. (n.d.). *Countering terrorism financing*.

Shaikh, A. K., Al–Shamli, M., & Nazir, A. (2021). Designing a relational model to identify relationships between suspicious customers in anti–money laundering (aml) using social network analysis (sna). *J Big Data*, *8*(1), 20. https://doi.org/10.1186/s40537-021-00411-3

Utkina, M. S., Reznik, O. M., & Bondarenko, O. S. (2023). The place and the role of financial monitoring in anti-money laundering system. *Eduvest*, *3*(5), 1019–1027. https://greenpublisher.id/

YANG, G. (2018). Crypto-assets and related some legal issues in financial industry. *The International*

Review of Financial Consumers, *3*(2), 1–8.

Yu, Q., Xu, Z., & Zong, K. (n.d.). Deep learning for cross-border transaction anomaly detection in anti-money laundering systems.