Mise en œuvre de règles de surveillance transactionnelle et analyse des alertes

Démarche d'initiation à la Lutte contre le blanchiment de capitaux et le financement du terrorisme

Théo Paradis

LinkedIn / email

Décembre 2025

1. présentation de la lutte contre le blanchiment

La Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LCB-FT) regroupe l'ensemble des dispositifs mis en place par les établissements financiers afin de prévenir, détecter et déclarer les opérations susceptibles de dissimuler l'origine illicite de fonds ou de contribuer au financement d'activités terroristes. Elle constitue un pilier essentiel du système financier, visant à garantir son intégrité et à lutter contre les flux financiers illicites.

Dans ce cadre, le rôle de l'analyste LCB-FT est central. Il intervient tout au long de la chaîne de surveillance transactionnelle en assurant un suivi constant des opérations réalisées par les clients. Son travail consiste à identifier des comportements financiers atypiques ou incohérents au regard du profil client, à analyser les flux et les schémas transactionnels, puis à interpréter les alertes générées par les outils de détection. À l'issue de cette analyse, l'analyste est en charge de qualifier les alertes, soit en les classant sans suite lorsqu'elles s'avèrent non pertinentes, soit en décidant de leur escalade lorsque les soupçons sont jugés fondés, notamment par le biais d'une déclaration de soupçon.

Ce poste implique une forte responsabilité réglementaire, car les décisions prises peuvent avoir des conséquences juridiques et financières importantes pour l'établissement. Il requiert également une capacité d'analyse approfondie, une grande rigueur, ainsi qu'une compréhension fine des typologies de blanchiment, des contraintes opérationnelles des clients et du cadre légal national et international encadrant la LCB-FT.

2. Présentation du projet et objectifs

Ce projet a été conçu comme un exercice pratique de mise en situation en Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LCB-FT). Il vise à reproduire, de manière simplifiée mais réaliste, les mécanismes fondamentaux de la surveillance transactionnelle mis en œuvre au sein des établissements financiers. L'approche retenue repose sur l'analyse de transactions à l'aide d'outils techniques et de règles de détection explicites, permettant de simuler le travail quotidien d'un analyste LCB-FT.

Les objectifs de ce projet sont doubles, dans un premier temps, il est question de développer des compétences techniques et analytiques en matière de détection des opérations suspectes. Cela inclut l'utilisation du langage Python pour la manipulation et l'analyse de données transactionnelles, la mise en place de règles de détection basées sur des seuils, ainsi que l'application d'une logique métier conforme aux principes de la LCB-FT. Et de Comprendre concrètement les enjeux du métier d'analyste LCB-FT, notamment le rôle de vigilance exercé face aux risques de blanchiment et de financement du terrorisme. Cette mise en situation permet d'évaluer l'adéquation entre les exigences opérationnelles de ce métier : une rigueur analytique, esprit critique, respect du cadre réglementaire et mes attentes professionnelles.

Le périmètre du projet a volontairement été maintenu simple et encadré, avec des règles de détection clairement définies. Ce choix méthodologique a été effectué afin de se concentrer sur les éléments essentiels de la surveillance transactionnelle, à savoir, la logique de détection des opérations potentiellement suspectes, la compréhension et l'application des seuils réglementaires, l'interprétation des résultats générés par les règles de surveillance, et le rôle opérationnel de l'analyste dans la prise de décision, incluant l'analyse des alertes et l'évaluation du niveau de risque.

Ainsi, ce projet constitue une première approche structurée et pédagogique de la surveillance LCB-FT, mettant en évidence l'équilibre nécessaire entre automatisation des contrôles et jugement humain dans l'analyse des transactions.

3. Présentation des bases de données

3.1. La base de données des transactions bancaires

La première base de données utilisée dans le cadre de ce projet a été générée artificiellement à l'aide de ChatGPT. Elle se compose d'une vingtaine d'observations, volontairement construites afin de représenter un large éventail de situations transactionnelles. Ces données synthétiques ont été élaborées de manière à couvrir les principaux cas de non-conformité rencontrés en LCB-FT, tout en incluant des opérations normales permettant de disposer d'un référentiel comparatif.

L'objectif de cette base de données n'est pas statistique ni prédictif, mais avant tout pédagogique. Elle vise à permettre une confrontation pratique à différents scénarios transactionnels, qu'ils soient conformes ou potentiellement suspects, afin de tester les règles de détection mises en place et d'en analyser les résultats.

Structure et variables principales

La base de données est structurée autour de plusieurs colonnes clés, chacune représentant une information essentielle à l'analyse LCB-FT :

transaction_id	client_id	date_transaction	type_transaction	montant_eur	pays_destination	contrepartie_id	sens	solde_apres_transaction
1	C04	2024-01-01	virement	3000	France	EXT05	OUT	97000
2	C08	2024-01-02	virement	2000	France	EXT11	OUT	98000
3	C01	2024-01-02	depot_cash	9500	France	NA	IN	12000
4	C05	2024-01-03	virement	50000	Luxembourg	EXT09	OUT	10000
5	C06	2024-01-04	depot_cash	3000	France	NA	IN	8000

- *transaction_id* : identifiant unique de la transaction, permettant d'assurer la traçabilité des opérations ;

- *client_id* : identifiant anonymisé du client à l'origine de la transaction, utilisé pour regrouper les opérations et analyser les comportements individuels ;

- *date_transaction* : date de réalisation de l'opération, indispensable pour l'analyse temporelle des flux financiers et l'application de fenêtres d'observation ;

- *type_transaction* : nature de la transaction (dépôt de liquidités, retrait de liquidités ou virement bancaire), permettant d'identifier les typologies spécifiques de risque ;

- *montant_eur* : montant de la transaction exprimé en euros, utilisé pour l'analyse des seuils réglementaires et des variations de montants ;

- *pays_destination* : pays vers lequel les fonds sont transférés ou pays de réalisation de l'opération, utilisé pour l'identification des flux internationaux et des zones à risque ;

- *contrepartie_id :* identifiant de la contrepartie externe à la transaction (bénéficiaire ou émetteur des fonds), absent pour les opérations en espèces, essentiel pour la détection des flux circulaires ;

- *sens* : sens du flux financier par rapport au compte du client (entrée ou sortie de fonds), permettant de distinguer les opérations de crédit et de débit ;

- *solde_apres_transaction* : solde du compte du client immédiatement après l'exécution de la transaction, utilisé pour analyser les variations de solde et les scénarios de transit rapide des fonds ;

Cette structure de données permet de reproduire, à une échelle réduite, les informations généralement disponibles dans les outils de surveillance transactionnelle.

3.2. La base de données “Know your customers”

La base de données KYC.csv regroupe des informations clients essentielles dans le cadre des obligations de connaissance du client (Know Your Customer – KYC).
Elle contient 10 clients décrits à travers 9 variables, couvrant à la fois des éléments d’identification, de profil économique et de comportement financier.

Cette base constitue un socle de données clients permettant d’évaluer, surveiller et classifier les risques LCB-FT.

client_id	type_client	profession	revenu_mensuel_estime	pays_residence	anciennete_relation_mois	usage_cash_attendu	flux_internationaux_habituels	niveau_risque_client
C01	Particulier	Restaurateur	4500	France	14	Élevé	Non	Élevé
C02	Particulier	Étudiant	1200	France	3	Faible	Non	Moyen
C03	Particulier	Consultant IT	6000	France	36	Faible	Oui	Moyen
C04	Professionnel	PME BTP	12000	France	60	Moyen	Non	Faible
C05	Professionnel	Holding patrimoniale	20000	France	48	Faible	Oui	Moyen
C06	Particulier	Auto-entrepreneur	3000	France	6	Moyen	Non	Moyen
C07	Particulier	Import-export	7000	France	24	Faible	Oui	Élevé
C08	Particulier	Cadre salarié	5500	France	72	Faible	Non	Faible
C09	Particulier	Investisseur privé	9000	France	18	Faible	Oui	Élevé
C10	Particulier	Employé	1800	France	1	Faible	Non	Moyen

La base de données est composée de plusieurs variables clés, chacune ayant un rôle spécifique dans le dispositif LCB-FT.

- *client_id:* correspond à l’identifiant unique du client et permet d’assurer la traçabilité ainsi que le suivi des opérations et du profil dans le temps.
- *type_client***:** indique s’il s’agit d’un particulier ou d’un professionnel ; cette distinction est essentielle pour adapter l’analyse et différencier les niveaux de risque.
- *profession:* renseigne sur l’activité ou le secteur du client et permet d’identifier d’éventuels secteurs sensibles ou exposés aux risques de blanchiment.
- *revenu_mensuel_estime***:** représente la capacité financière estimée du client et sert à détecter d’éventuelles incohérences entre les revenus déclarés et les flux financiers observés.
- *pays_residence:* indique le pays de résidence du client et permet d’analyser le risque géographique, notamment en lien avec les juridictions à risque élevé.
- *L’anciennete_relation_mois:* mesure la durée de la relation bancaire ; les relations récentes étant généralement considérées comme plus risquées en matière de LCB-FT.
- *usage_cash_attendu:* décrit le niveau attendu d’utilisation d’espèces, un élément clé de surveillance puisque le cash constitue un vecteur privilégié de blanchiment de capitaux.
- *flux_internationaux_habituels***:** indique la présence ou non de flux transfrontaliers, permettant d’identifier des risques liés aux opérations internationales.

- *niveau_risque_client:* correspond au niveau de risque attribué au client (faible, moyen ou élevé) et sert de base à la mise en œuvre d'une vigilance adaptée ou renforcée.

4. Structure du projet et règles de détection

Le projet repose sur un ensemble de règles de détection inspirées des principes de la réglementation LCB-FT ainsi que des recommandations internationales, notamment celles du Groupe d'Action Financière (GAFI) et des directives européennes. Ces règles ont été volontairement conçues de manière explicite et transparente afin de faciliter leur compréhension et leur interprétation.

L'objectif est de mettre en évidence quelques typologies clés de blanchiment, fréquemment rencontrées en pratique.

4.1 Détection du Smurfing

Principe
Le smurfing est une technique de blanchiment consistant à fractionner des dépôts en espèces en plusieurs opérations de faible montant, réalisées sur une période courte, dans le but d'éviter les seuils de vigilance réglementaires.

Seuils retenus
Les critères suivants ont été retenus pour identifier un schéma de smurfing :

- Des montants unitaires inférieurs à 10 000 € ;
- Un minimum de cinq transactions ;
- Une période d'observation de sept jours.

Ces seuils sont cohérents avec les obligations de vigilance prévues par la réglementation européenne en matière de contrôle des opérations en espèces.

4.2 Transactions vers des pays à risque

Certaines transactions présentent un niveau de risque accru en raison de la destination des fonds, notamment lorsqu'elles concernent des pays caractérisés par :

- Des régimes de surveillance et de contrôle insuffisants ;
- L'existence de sanctions internationales ;
- Un niveau élevé de criminalité financière.

Dans ce projet, un seuil de 5 000 € a été retenu afin de cibler les flux financiers significatifs à destination de ces juridictions. La liste des pays considérés comme à risque s'appuie sur des classifications internationales reconnues (GAFI, Union européenne).

4.3 Détection du cash in / cash out rapide

Principe
Un schéma de cash in / cash out rapide correspond à un dépôt de fonds suivi d'un retrait dans un délai très court. Ce comportement peut indiquer une tentative de blanchiment visant à réintroduire rapidement des fonds d'origine illicite dans le circuit financier.

Seuil retenu
Le critère retenu dans le cadre de ce projet est un délai maximal de 24 heures entre l'entrée des fonds (cash in) et leur sortie (cash out).

5. Résultats et interprétation des alertes

À l'issue de l'application des règles de surveillance transactionnelle, plusieurs alertes ont été générées via *transactions_suspectes.csv*. Leur analyse ne peut toutefois être menée de manière isolée : conformément à l'approche par les risques préconisée par le GAFI et reprise par le Code monétaire et financier (articles L.561-1 et suivants), chaque alerte doit être interprétée à la lumière du profil KYC du client, de son historique et de la cohérence globale de ses opérations.

transaction_id	client_id	date_transaction	type_transaction	montant_eur	pays_destination	contrepartie_id	sens	solde_apres_transaction	reason
3	C01	2024-01-02	depot_cash	9500	France		IN	12000	Smurfing (depots cash fractionnes)
7	C01	2024-01-03	depot_cash	9800	France		IN	21800	Smurfing (depots cash fractionnes)
11	C01	2024-01-04	depot_cash	9700	France		IN	31500	Smurfing (depots cash fractionnes)
18	C01	2024-01-05	depot_cash	9600	France		IN	41100	Smurfing (depots cash fractionnes)
21	C01	2024-01-06	depot_cash	9400	France		IN	50500	Cash in / cash out rapide
25	C01	2024-01-07	virement	48000	France	EXT01	OUT	2500	Cash in / cash out rapide
9	C02	2024-01-10	depot_cash	20000	France		IN	21000	Cash in / cash out rapide
14	C02	2024-01-11	virement	19500	France	EXT02	OUT	1500	Cash in / cash out rapide
6	C03	2024-01-05	virement	15000	Nigeria	EXT03	OUT	3000	Transaction vers pays a risque
4	C05	2024-01-03	virement	50000	Luxembourg	EXT09	OUT	10000	Transaction vers pays a risque
5	C06	2024-01-04	depot_cash	3000	France		IN	8000	Cash in / cash out rapide
17	C06	2024-01-05	retrait_cash	2800	France		OUT	5200	Cash in / cash out rapide
12	C09	2024-01-10	virement	9000	Iles Caimans	EXT15	OUT	2000	Transaction vers pays a risque

Client C01 — Dépôts fractionnés en espèces (structuration)

Analyse :
Le client C01 exerce une activité de restauration, ce qui implique un recours légitime et attendu aux espèces. Son profil KYC indique un usage du cash élevé. Toutefois, l'analyse transactionnelle met en évidence cinq dépôts en espèces sur une période de cinq jours, pour des montants systématiquement proches mais inférieurs au seuil de 10 000 euros. Ce schéma correspond à une typologie classique de structuration visant à éviter les seuils de vigilance.
Par ailleurs, ces dépôts sont suivis d'un virement sortant représentant la quasi-totalité du solde du compte vers une contrepartie non identifiée, ce qui renforce le caractère atypique de la séquence.

Décision:
Malgré une activité partiellement compatible avec l'usage d'espèces, la fréquence, le calibrage des montants et la sortie rapide des fonds dépassent ce qui est attendu au regard du profil client. L'alerte est jugée pertinente et doit être escaladée pour analyse approfondie par le service conformité, avec un risque de déclaration de soupçon à TRACFIN.

Client C02 — Cash in / cash out rapide

Analyse:
Le client C02, étudiant avec un revenu mensuel estimé faible et une ancienneté de relation bancaire récente, a reçu un dépôt en espèces de 20 000 euros alors que son solde initial était limité. Le lendemain, un virement sortant de 19 500 euros est observé vers une contrepartie non identifiée. Les montants entrants et sortants sont quasi équivalents, laissant apparaître une faible rétention des fonds sur le compte.

Décision:
Ce schéma est caractéristique d'un mécanisme de transit rapide des fonds (cash in / cash out), difficilement compatible avec le profil économique déclaré du client. L'alerte est confirmée et nécessite une escalade en vue d'un examen renforcé.

Client C03 — Virement international vers le Nigeria

Analyse:
Le client C03 exerce une activité de consultant IT et présente une ancienneté significative, avec des flux internationaux habituels déclarés dans son profil KYC. Le virement à destination du Nigeria, pays classé à risque par les instances internationales, déclenche néanmoins une alerte légitime.

Toutefois, la nature de l'activité du client peut justifier des relations économiques avec des juridictions étrangères, y compris à risque.

Décision:
L'alerte ne peut être automatiquement qualifiée de suspecte. En l'absence d'éléments justificatifs complémentaires, elle doit faire l'objet d'une vigilance renforcée, conformément au principe de proportionnalité. Une demande d'informations supplémentaires est nécessaire avant toute conclusion définitive.

Client C05 — Flux circulaires via une contrepartie étrangère

Analyse:
Le client C05 est une holding patrimoniale présentant des flux internationaux habituels. Un virement important est effectué vers le Luxembourg, juridiction non classée à risque par le GAFI. Toutefois, les fonds reviennent ultérieurement sur le compte du client via la même contrepartie, pour un montant proche, sans justification économique apparente.

Décision:
Le risque ne repose pas sur la destination géographique, mais sur la rotation rapide et circulaire des fonds, typologie fréquemment associée à des mécanismes de blanchiment. L'alerte est jugée pertinente et nécessite une analyse approfondie.

Client C06 — Entrée et sortie rapide de fonds en espèces

Analyse:
Le client C06, auto-entrepreneur avec une ancienneté limitée, a reçu un dépôt en espèces de 3 000 euros, suivi dès le lendemain d'un retrait ou virement d'un montant très proche. La faible variation de solde peut correspondre à une commission conservée par le client. Le profil KYC indique un usage du cash seulement modéré.

Décision:
Ce comportement est caractéristique d'un schéma de cash in / cash out sans conservation durable des fonds. L'alerte est confirmée et doit être traitée comme pertinente.

Client C09 — Virement vers les Îles Caïmans

Analyse:
Le client C09 a réalisé un virement à destination des Îles Caïmans, territoire associé à des risques élevés d'opacité financière et de structures offshore. Bien que le client présente un profil

d'investisseur privé avec des flux internationaux déclarés, l'absence d'identification claire de la contrepartie et le contexte géographique renforcent le niveau de risque.

Décision:
Conformément aux obligations de vigilance renforcée prévues par le Code monétaire et financier, cette opération doit faire l'objet d'une analyse approfondie. L'alerte est maintenue et nécessite un examen complémentaire.

6. Ouverture – Limites du projet et enjeux opérationnels

Bien que ce projet permette de reproduire les mécanismes fondamentaux de la surveillance transactionnelle en LCB-FT, il reste volontairement simplifié et présente certaines limites inhérentes à son périmètre pédagogique. L'introduction de variables KYC enrichit l'analyse et permet de contextualiser les alertes, mais elle ne reproduit pas encore la complexité totale d'un environnement opérationnel réel.

6.1 Scoring et hiérarchisation des alertes

Dans un cadre opérationnel, chaque alerte est généralement pondérée via un système de scoring combinant plusieurs critères : montant, fréquence, profil client, historique de transactions, flux internationaux, niveau de risque du pays de destination, etc.
Le présent projet ne met pas en place de scoring automatique, mais l'intégration de la dimension KYC constitue une base méthodologique solide pour une hiérarchisation future des alertes. L'ajout de cette information permet déjà de distinguer les faux positifs des alertes pertinentes selon le contexte client et de prioriser les investigations.

6.2 Faux positifs : causes et limites

La génération de faux positifs reste un défi majeur dans la surveillance LCB-FT. Même avec l'enrichissement KYC, certains flux peuvent être signalés malgré leur légitimité :

- Activité économique normale correspondant au profil KYC (commerçants, professions manipulant des liquidités, investisseurs privés) ;
- Flux internationaux habituels pour certains clients justifiés par leur activité ;
- Dépôts ou retraits saisonniers liés à des périodes spécifiques (fêtes, soldes) ;
- Seuils de détection volontairement sensibles pour l'exercice pédagogique.

Ces éléments montrent l'importance d'un ajustement continu des règles de détection, ainsi que de l'utilisation systématique des informations KYC pour réduire les faux positifs et améliorer la pertinence des alertes.

6.3 Faux négatifs : un risque majeur

Les faux négatifs, c'est-à-dire les opérations suspectes non détectées, constituent un risque critique. Ils peuvent résulter de :

- Contournements intelligents des seuils réglementaires ;
- Schémas fractionnés répartis sur plusieurs comptes ou dans le temps ;
- Comportements clients évolutifs difficiles à anticiper.

La réduction de ces risques nécessite une analyse plus sophistiquée, incluant scoring avancé, analyses comportementales longitudinales et interprétation humaine. L'ajout de variables KYC dans ce projet est un premier pas vers une approche plus réaliste, permettant de mieux identifier les alertes réellement pertinentes.

7. Conclusion et bilan personnel

Ce projet constitue pour moi une immersion concrète et structurée dans l'environnement de la conformité bancaire, enrichie par l'intégration des informations KYC. L'objectif initial était de comprendre le métier d'analyste LCB-FT et d'évaluer mon intérêt pour ce domaine.

J'ai particulièrement apprécié la transformation des règles réglementaires abstraites en outils concrets de détection et l'analyse approfondie des flux, intégrant à la fois les typologies de blanchiment et le profil des clients. L'exercice m'a permis de mesurer l'importance du jugement humain dans la qualification des alertes et de comprendre la nuance nécessaire pour distinguer faux positifs et alertes pertinentes.

Cette expérience a conforté mon choix de carrière : je souhaite désormais obtenir une première expérience professionnelle en banque ou en cabinet spécialisé. Les aspects les plus stimulants restent à venir, notamment l'interprétation fine des flux complexes, la hiérarchisation des alertes, et la mise en œuvre concrète des obligations réglementaires. Ce travail m'a donné un aperçu précieux de l'investigation complexe au cœur de la lutte contre le blanchiment de capitaux et le financement du terrorisme.