



# Échange d'informations entre les banques et les autorités réglementaires et lutte contre la criminalité financière

EL GNAOUI Leila (1); RAOUI Abderrahim (2) ; BENJELLOUN Amine (3)

(1) Professeure universitaire

(2) et (3) : Doctorants en sciences de gestion

Laboratoire Business Intelligence, Gouvernance des organisations, Finance et Criminalité financière (BIGOFCE)

Faculté des sciences juridiques économiques et sociales Ain Chok Casablanca.

Université HASSAN II Casablanca Maroc

**Résumé :** Notre article a pour objectif d'étudier la contribution de l'échange d'informations entre les banques et les autorités réglementaires dans la lutte contre les crimes financiers et dans quelle mesure les nouvelles technologies peuvent assurer le renforcement de cette coopération.

Notre travail a été élaboré avec une méthode de recherche quantitative traduite par un questionnaire qui a été adressé aux responsables des fonctions des banques et dont principalement l'audit interne, le contrôle permanent, et la sécurité financier des banques, en plus des responsables de Bank Al Maghrib (Banque Centrale du Maroc) et de l'Autorité Nationale du Renseignement Financier (ANRF). Les résultats de l'étude ont mis en évidence l'importance du partage d'informations entre les établissements bancaires et les autorités réglementaires et son rôle en matière de lutte contre les crimes financiers.

Elle met l'accent sur la nécessité de promouvoir les modalités d'investigations et de communication destinées à :

- Dynamiser les processus du partage d'informations ;
- Optimiser le contrôle des flux financiers illicites et appuyer les actions des poursuites judiciaires ;
- Préserver la confiance et assurer l'intégrité et de l'institution bancaire.

Outre l'intérêt de l'échange d'informations, notre article examine les défis et les opportunités associés à ce partage d'informations.

Nous estimons que les principales conclusions de notre recherche peuvent avoir des implications consistantes sur le plan opérationnel de lutte contre les crimes financiers au niveau des banques et en particulier sur les mécanismes des mesures de contrôle, de signalement et de coopération entre les acteurs de référence.

**Mots-clés :** Echange d'informations ; Banque ; Autorités réglementaires ; Lutte contre la criminalité financière ; Détection des activités criminelles ; Nouvelles technologies.

**Digital Object Identifier (DOI):** <https://doi.org/10.5281/zenodo.11476190>

**Published in:** Volume 3 Issue 3



This work is licensed under a [Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License](https://creativecommons.org/licenses/by-nc-nd/4.0/).

## **Introduction :**

L'échange d'informations représente un élément clé de la réglementation du système bancaire et constitue une base de toute collaboration entre les banques et les autorités réglementaires.

Il a pour principale finalité de partager les informations liées à l'identification des clients des banques, au fonctionnement de leurs comptes et aux incidents et risques associés à leurs transactions.

Afin d'éviter toute complicité dans des activités illicites ou de mettre en cause leur responsabilité, les banques priorisent le traitement des risques des crimes financiers liés aux transactions bancaires conformément aux exigences et des obligations de vigilance entourant la relation client.

D'un point de vue opérationnel, l'environnement bancaire offre des conditions propices aux diverses formes de la délinquance financière et peut faciliter la création des circuits financiers illégaux.

Les protagonistes criminels mettent au point diverses méthodes pour faciliter l'infiltration de capitaux illégaux dans le système bancaire et dissimuler leur origine en recourant à des techniques d'empilement et de multiplication des transactions. Ce qui peut rendre complexe et difficile leur détection en conséquence. Cette situation se traduit par la multiplication et l'interconnexion des circuits financiers criminels, et en particulier par l'ampleur des risques au niveau international.

A cet effet, le partage d'informations et la collaboration étroite entre les banques et les autorités réglementaires s'avère importante pour détecter les activités illicites et de permettre la résolution des enjeux associés à la criminalité financière.

Conformément à une étude de Quintel Teresa (2022) et en conformité aux règles du GAFI, l'échange d'informations entre les banques est déterminant pour combattre de manière efficace les crimes financiers et en particulier le blanchiment des capitaux.

Dans ce sens, le partage d'informations permet d'avoir une vision exhaustive des activités suspectes de la clientèle ; Ce qui permet de mieux repérer les schémas criminels transfrontaliers et de contribuer à la sécurité des systèmes financiers.

Cet échange revêt une importance capitale car il permet d'approfondir une meilleure compréhension des clients des banques et des processus des activités illicites transitant par les circuits bancaires. Cet outil opérationnel devrait faciliter l'exploration des actes criminels liés aux activités et des processus bancaires grâce à des signalements et à la diffusion des données.

Le partage des données entre les établissements bancaires et les autorités de régulation revêt un caractère capital compte tenu de la complexité et l'évolution de la criminalité financière, dans la mesure où il permet de :

- Optimiser les modalités d'investigation des risques criminels financiers ;
- Piloter la surveillance des flux financiers illicites et encourager les poursuites judiciaires les concernant ;
- Améliorer et enrichir la base des données des cellules nationales des renseignements financiers.

Sur le plan international, cet échange permet aux banques de contribuer de manière active à la lutte contre l'opacité transfrontalière et de préserver la résilience des systèmes financiers

Dans cette optique notre recherche est axée sur la problématique suivante :

**Dans quelle mesure l'échange d'informations entre les banques et les autorités réglementaires peut contribuer à la lutte contre la criminalité financière ?**

L'optimisation de cet échange et la prévention de la délinquance financière constituent un enjeu majeur pour les stratégies de la gouvernance bancaire.

Aussi la capacité de cette coopération peut-elle être renforcée par l'émergence des nouvelles technologies financières.

Plusieurs questions de recherche sont associées à cette thématique et portent sur les points suivants :

- Dans quelle mesure la collaboration entre les banques et les autorités réglementaires peut faciliter la détection des activités financières illicites ?
- Quelles sont les normes de communication appropriées pour faciliter les échanges d'informations ?

- Quels sont les moyens exploités par les banques pour appuyer la coordination en matière de lutte contre la criminalité financière à l'échelon international ?

Le développement des programmes de prévention reste tributaire d'un échange accru des données, de l'engagement et de l'adaptation des parties concernées à l'évolution technologique et des pratiques complexes des crimes financiers.

Cette régulation reste tributaire de la mise à niveau du cadre réglementaire régissant la sécurité financière et la conformité des banques.

Notre recherche a pour objectifs de mettre le point sur :

- Les processus opérationnels de gestion et les standards exploités pour faciliter l'échange sécurisé des données ;
- Les modalités du suivi de l'échange d'information et de la supervision de la criminalité financière ;
- La formulation des recommandations pour appuyer les mesures opérationnelles de coopération et maîtriser les risques associés à l'évolution technologique et des activités criminelles.

Notre article abordera, outre le contexte conceptuel et théorique :

- L'état des lieux et la gestion des dispositifs de coopération entre les banques et les autorités de régulation en matière du partage d'informations liées à la criminalité financière ;
- Les opportunités, les contraintes et les défis de l'échange des informations ;
- La contribution de l'échange d'information à la lutte contre la criminalité financière.

Notre étude est appuyée par une recherche empirique destinée à analyser la problématique retenue par nos soins, examiner les questions y associées et apprécier des hypothèses retenues pour notre analyse pratique. Notre travail est élaboré avec une méthodologie de recherche quantitative traduite par un questionnaire adressé aux responsables des fonctions de la sécurité financière des banques, de l'audit interne, du contrôle permanent, du système d'information des banques en plus des responsables de Bank Al Maghrib et de l'Autorité Nationale du Renseignement Financier (ANRF).

## **1. Contexte et enjeux de l'échange d'informations entre les banques et les autorités réglementaires :**

### **1.1. Contexte de l'échange d'informations entre les banques et les autorités réglementaires :**

#### **1.1.1. Cadre théorique de l'échange d'informations entre les banques et les autorités réglementaires :**

Le cadre conceptuel de notre recherche peut être appréhendé sur la base des trois notions clés ci-après définies :

→ L'échange d'informations :

L'échange d'informations par les banques se manifeste par le partage avec les autorités de régulation des données portant sur les activités de leur clientèle dans le but d'assurer la détection des éventuels flux financiers illicites.

Dans ce contexte, les informations échangées peuvent porter sur :

- L'identification de la clientèle et des bénéficiaires effectifs des transactions financières suspectes afin de tracer les processus des flux financiers éventuels ;
- Les activités suspectes ou inhabituelles sur les comptes bancaires en tant que signaux forts du blanchiment des capitaux ou du financement du terrorisme ;
- Les informations sur les transactions avec des pays sanctionnés ;
- Les informations sur les transactions impliquant des personnes politiquement exposées (PPE) susceptibles de présenter des risques importants de corruption ;
- Les informations sur les fraudes et les escroqueries financières quoique leurs nombres soient moins élevés.

Compte tenu de leurs obligations légales, les banques sont tenues d'assurer la déclaration de toute transaction douteuse ou suspecte au regard du profil du client. Cette démarche permet aux autorités réglementaires de disposer d'une vision exhaustive des mouvements financiers en cause.

Conformément aux dispositions de l'article 9 de la loi marocaine n° 43-05 régissant la lutte contre le blanchiment des capitaux, les banques doivent communiquer à l'ANRF la liste des personnes habilitées à faire des déclarations des soupçons liés aux opérations et au profil de la clientèle.

Les déclarations des soupçons sont diligentées sur la base d'un modèle approprié mis en place par l'ANRF devant contenir des informations complètes sur le client, ses biens, ses opérations, le détail des soupçons relevés et les actions entreprises par les banques.

La déclaration par les banques des opérations des clients suspectés peut impliquer plusieurs problèmes et obstacles dont notamment :

- La connaissance insuffisante des formes et des procédés de la criminalité financière ;
- Le nombre croissant des transactions de la clientèle et leur complexité ;
- Les préoccupations juridiques et réglementaires liées à la sécurité et à la confidentialité des données de la clientèle ;
- Le coût des ressources allouées aux dispositifs de surveillance ;
- Les contraintes de coordination entre les établissements bancaires et les autorités de régulation.

Aussi, les banques sont tenues par les obligations de la protection et la confidentialité des données personnelles de leurs clients lors de tout échange avec les autorités de régulation.

→ La criminalité financière :

La criminalité financière couvre toutes les activités illicites visant à bénéficier des fonds indus et à un enrichissement personnel par des moyens de fraude.

La criminalité financière peut prendre différentes formes au niveau du secteur bancaire : fraude, corruption, conflits d'intérêts, blanchiment de capitaux, financement du terrorisme, escroquerie etc.

La lutte contre la criminalité financière constitue un élément clé de la stratégie et des plans d'action de la gouvernance bancaire.

La détection et l'identification des flux financiers illicites nécessitent des capacités d'analyse et d'investigation avancées et obligent les banques à déployer des compétences spécifiques pour assurer le contrôle et le suivi des opérations à risque.

→ Le renseignement financier :

Le renseignement financier consiste à collecter et analyser les données en rapport avec les opérations des clients des banques et des mouvements financiers de leurs comptes.

L'analyse de ces données est assurée sur la base des croisements et des recoupements afin d'identifier et de retracer les flux frauduleux potentiels au niveau des processus bancaires.

Ce travail d'analyse est appuyé par des investigations et des appréciations personnalisées.

La production du renseignement financier donne lieu à une diffusion aux services répressifs en charge des enquêtes.

Pour l'examen du cadre théorique de notre recherche nous avons retenu les trois théories scientifiques mobilisées suivantes :

→ La théorie de l'agence qui examine les relations principal-agent et le traitement des problématiques liées à l'asymétrie d'information notamment les déséquilibres informationnels pouvant affecter la qualité de l'échange.

→ La théorie des coûts de transaction qui analyse les coûts et les avantages de leur réduction via la confiance et les processus de normalisation du partage des données entre les deux parties.

→ Le modèle d'acceptation des technologies TAM évalue l'impact de la facilité d'utilisation et de l'utilité perçues des technologies sur l'acceptation par les banques et autorités de solutions améliorant les échanges.

Ce modèle analyse les leviers psychologiques et organisationnels permettant d'améliorer l'adoption des solutions technologiques proposées par les autorités pour renforcer les échanges et lutter contre la criminalité financière dans le respect des réglementations.

L'échange d'informations entre les banques et les autorités réglementaires a pour principaux objectifs de :

- Protéger les intérêts, les avoirs et les données personnelles de la clientèle des banques ;
- Obtenir le renseignement financier par le biais de la collecte et l'analyse des données ;
- Lutter contre la criminalité financière sur la base de la détection des flux financiers illicites, la prévention et la répression des fraudes ;
- Renforcer les mesures de la dissuasion et de la répression des menaces ;
- Consolider la coopération internationale en raison de la dimension transfrontalière des infractions.

### **1.1.2. Contexte réglementaire et légal de l'échange d'informations entre les banques et les autorités réglementaires :**

Les banques sont tenues par des obligations liées à la divulgation régulière des informations, aux reportings réglementaires, à la confidentialité et à la protection des données personnelles de leur clientèle.

Le contexte réglementaire marocain (Loi bancaire, Code du commerce et...) définit les règles régissant les activités bancaires et encadre les échanges d'informations entre les banques et les autorités réglementaires.

Ce cadre législatif repose sur le respect des pouvoirs, devoirs et responsabilités des autorités réglementaires et des banques régissant l'échange des données.

Par ailleurs les autorités réglementaires sont dotées des prérogatives spécifiques qui leur permettent de collecter les données des banques tout en recourant à leurs pouvoirs en matière de supervision et de sanction.

Les mécanismes de coordination et d'échange mis en œuvre au niveau des banques sont conçus pour se conformer et respecter les dispositions réglementaires et légales.

Au niveau international, les accords et les normes internationaux sont promulgués essentiellement dans le but de promouvoir la coordination de l'échange d'informations.

Sur le plan international, l'échange d'informations est organisé et réglementé grâce à l'intervention et aux actions des différents organismes financiers à vocation internationale tels que le GAFI, le FMI, l'ONU, l'OCDE etc.

Dans ce contexte, des conventions sont signées par les pays membres de ces organismes pour faciliter le partage des données entre leurs autorités nationales en vertu des accords bilatéraux.

La coordination des échanges sur le plan international se caractérise par le respect des règles de protection sécurité et confidentialité des données.

Le GAFI en tant qu'autorité internationale a formulé aux institutions bancaires une série de recommandations visant à optimiser l'échange efficace des informations et en particulier :

- Souligner l'utilité du partage au sein du secteur privé, et principalement les banques, pour renforcer l'efficacité des mesures préventives ;
- Clarifier les normes du GAFI relatives au partage au sein des groupes et entre institutions distinctes ;
- Identifier les principaux défis et les obstacles du partage au sein des groupes et entre les institutions concernées.

Conformément aux normes du GAFI, le partage efficace d'informations est déterminant pour optimiser l'allocation des ressources des banques et des autorités sur la base d'une approche quantitative et qualitative des menaces et parfaire toute coordination entre parties prenantes (FATF2012).

Toutefois, certaines entraves peuvent affecter les modalités du partage d'informations et générer des points d'incertitude d'ordre juridique et réglementaire (FATF2017).

A l'instar de l'ONU et du GAFI, une attention particulière est accordée par le comité de BALE à l'utilisation abusive du système financier international, au financement du terrorisme, et sa prévention grâce au partage transfrontalier d'informations financières. (Comité de BALE Avril 2002).

### **1.1.3 Contexte organisationnel de l'échange des informations liées à la criminalité financière entre les banques et les autorités réglementaires :**

L'échange d'informations permet de contribuer à une meilleure gestion des risques et d'assurer l'efficacité des dispositifs de lutte contre le blanchiment des capitaux et le financement du terrorisme (FATF : 2017).

### **1.1.3.1. Modalités d'organisation d'échange d'informations :**

Les normes consolidées du GAFI, datées de 2016 clarifient les exigences en matière du partage d'informations.

De ce fait, les banques collectent et partagent les informations sur leurs clients et les types identifiés des transactions en vertu des réglementations mises en place.

Elles ont l'obligation de signaler les transactions suspectes aux autorités réglementaires. Ces dernières peuvent solliciter de manière ponctuelle aux banques des éléments ou des informations déterminées sur un client précis ou son compte bancaire.

Pour organiser cette action, les normes du GAFI visent à établir un cadre formel garantissant un partage concerté des informations efficaces entre les autorités chargées de la supervision prudentielle des activités bancaires et les cellules du renseignement financier.

Le partage d'informations doit être assuré conformément à des règles prédéfinies.

Selon le GAFI, les modalités d'organisation, de communication et du suivi de l'échange doivent obéir à des critères de pertinence des informations partagées (FATF : 2017).

En conformité avec les dispositions de la recommandation numéro 20 du GAFI, le partage d'informations et la déclaration des transactions suspectes doivent être assurés avec toute la confidentialité requise pour son bon fonctionnement et le respect des mesures de leur protection.

Les informations partagées doivent être jugées pertinentes par la fonction conformité du groupe (bancaire) pour les besoins d'une meilleure gestion des risques BC/FT au niveau du groupe. (FATF : 2017).

L'échange d'informations est assuré en bonne partie de manière automatique et sécurisée et porte sur les données liées à l'identification des clients ou de leurs transactions et ce pour un examen approfondi des flux suspects.

Des mécanismes de supervision, reporting, audits et mesures dissuasives doivent être mis en place pour garantir la transparence et le respect de la réglementation en matière du partage d'informations (Quintel, Teresa : 11 Janvier 2022).

Les plateformes de partage d'informations sont conçues pour optimiser la détection des risques des crimes financiers tout en opérant des rapprochements et des recoupements des informations. L'exploitation de ces plateformes assure une gestion plus efficace et proactive des risques grâce à une vision élargie et une compréhension partagée avec l'ensemble des parties prenantes.

Le contexte organisationnel de l'échange des informations peut varier en fonction des dispositions réglementaires le régissant.

En vertu de ces règles, les structures mises en place doivent permettre de faciliter le partage sécurisé des informations et de superviser la conformité des banques.

### **1.1.3.2. Description des plateformes d'échange d'information entre les banques et les autorités en charge du traitement du renseignement financier :**

Sur le plan opérationnel, plusieurs niveaux de partage sont possibles au sein d'un groupe bancaire et ont pour objectifs de garantir un échange efficace de données quel que soit le modèle organisationnel adopté.

Sur le plan pratique, les plateformes mises en place au niveau du secteur bancaire constituent des outils clés pour promouvoir la transparence et contrer les activités financières illicites.

Ces plateformes sont dédiées essentiellement, au partage d'informations entre les banques et les autorités réglementaire (Autorité Nationale du Renseignement Financier ANRF et Bank Al Maghrib etc.).

Les plateformes mises en place assurent à titre principal, la déclaration des transactions suspectes aux autorités de régulation.

Elles permettent la production des informations détaillées relatives aux opérations de la clientèle, y compris les noms des parties impliquées, les montants, les dates et les motifs de suspicion.

Au Maroc l'échange d'informations entre les banques et l'ANRF est assuré par l'exploitation et la mise en œuvre d'un programme informatique intitulée « GO AML » institué par l'Office des Nations Unies contre la Drogue et le Crime (ONU DC).

Ce dispositif est doté d'une base des données intégrée et d'un système d'analyses développé par le programme onusien de modélisations et d'innovations technologiques d'aide à la lutte contre la corruption et la criminalité financière. (<https://unite.un.org/goaml/fr/content/description>).

L'application « GO AML » est exploitée via une plateforme dédiée de l'ANRF et remplit les fonctions principales de collecte et d'analyse des données.

Cette application permet d'effectuer à titre principal :

- Les déclarations de soupçons émises par les banques sur toutes les infractions sous-jacentes au blanchiment de capitaux et au financement du terrorisme ;
- Les demandes d'informations de l'ANRF aux banques (sur les personnes physiques ou morales) et leurs transactions au cours d'une période spécifiée dans la demande de l'ANRF ;
- Les demandes d'informations de fiabilisation (avec demande des références des cartes identités nationales et des fichiers électroniques de relations clientèle).

Elle permet également d'échanger les données entre les cellules du renseignement financiers, les banques, les autres personnes assujetties, les autorités judiciaires et les organismes régionaux ou internationaux.

D'autre part, les banques utilisent une deuxième plateforme intitulée « CNASNU » qui permet d'assurer le partage d'informations avec la Commission Nationale chargée de l'application des sanctions prévues par les Résolutions du Conseil de Sécurité des Nations-Unies relatives au terrorisme, à la prolifération des armes et à leur financement. (<https://cnasnu.justice.gov.ma/language/fr/accueil>).

En pratique, cette plateforme est dédiée au partage des données sur l'opérationnalisation du gel des avoirs et des biens pour les clients figurant sur les listes diffusées des sanctions annexées aux Résolutions du Conseil de Sécurité des Nations-Unies relatives au terrorisme, à la prolifération des armes et à leur financement.

La mise en place et l'exploitation des dispositifs du partage d'informations entre les banques et les autorités réglementaires accordent une importance particulière aux aspects primordiaux et à la sensibilité des informations échangées dont en particulier :

- La sécurité des données pour protéger les données contre les accès non autorisés, les fuites ou les cybers attaques ;
- La confidentialité et la protection des données traitées conformément aux dispositions des lois et des règles en matière de protection des données personnelles ;
- La communication des systèmes d'information existants et la fluidité des informations partagées.

Les plateformes d'échange d'information facilitent la coordination, et garantissent la transparence et l'efficacité de détection et de prévention de la criminalité financière au niveau des banques.

Toutefois la mise en œuvre des plateformes d'échange soulève des défis et des enjeux d'ordre technique, organisationnel et réglementaire.

La gestion de ces plateformes est confrontée à des contraintes et aux exigences de coopération internationale à la fois cruciale et complexe.

Selon le Comité de Bâle, un système centralisé d'évaluation des risques liés au partage des données au sein des groupes bancaires est jugé important.

La gestion des problématiques et la réponse aux contraintes nécessitent une concertation et une coordination efficace entre les banques et les autorités réglementaires de tutelle.

## **1.2. Déterminants et exigences d'efficacité de l'échange d'informations entre les banques et les autorités réglementaires :**

Un échange solide et performant d'informations doit être basé sur une crédibilité partagée et une confiance réciproque qui définissent et régissent les relations des banques et des autorités chargées de la supervision bancaire.

Cette exigence clé est jugée utile pour faciliter un partage sécurisé et transparent des informations.

Pour les besoins de sécurité juridique des échanges, les liens entre les banques et les autorités réglementaires doivent être régis par un cadre légal et réglementaire contraignant avec une définition précise des obligations de chaque partie en matière d'échange des données.

Les dispositions réglementaires doivent faire l'objet d'une refonte impérative et prendre en considération les défis liés à l'exploitation des plateformes d'échange.

Le partage d'informations joue un rôle clé en matière de détection et de compréhension des flux financiers illicites dans le secteur bancaire.

A cet effet, les dispositifs techniques de coordination mutuelle constituent des outils efficaces pour le partage d'informations.

La collaboration Banques /Autorités de régulation favorise l'amélioration des capacités d'analyse des risques grâce au partage réciproque de leurs connaissances, des solutions technologiques et l'adoption des mesures de prévention et de correction efficaces.

Le bon fonctionnement de ce processus doit prendre en considération les contraintes liées :

- Aux enjeux de confidentialité et de protection des données robustes ;
- A la multiplication des dispositions juridiques et les obstacles ayant trait à la coopération internationale entre pays ;
- A la complexité technique associée à l'hétérogénéité des systèmes informatiques.

Le partage des informations doit être régi par des dispositifs juridique et organisationnel fiables pour assurer sa conformité par rapport aux lois en vigueur.

Toutefois, la pratique de l'échange d'informations peut-être impactée par des obstacles d'ordre opérationnel ou juridique en mesure de freiner la disponibilité, l'accès, le partage et le traitement des informations liées à la lutte contre les crimes financiers.

Selon le GAFI, le partage d'informations implique des problématiques potentielles liées à l'insuffisance d'implication des autorités publiques ou au manque de coordination en rapport avec la protection des données etc.

La représentation commune du rôle de chaque acteur dans la lutte contre la criminalité économique est essentielle.

A ce sujet, le GAFI a identifié six facteurs clés pour soutenir cette vision partagée : leadership commun, engagement pour l'intégration des données, implication des forces de l'ordre, traitement des données personnelles, acceptation du public, soutien international (GAFI).

Selon une étude sur les règles de protection des données applicables aux cellules du renseignement financier élaborée par Quintel, T en 2022, l'échange performant d'informations obéit à des exigences d'efficacité dont nous citons :

- La considération des règles régissant le caractère confidentiel des données et le secret professionnel ;
- Le déploiement des dispositifs techniques adaptés pour un partage automatisé des informations ;
- La confidentialité et la protection des données par des canaux sécurisés ;
- L'utilisation encadrée des informations pour les besoins des missions de contrôle et d'investigation des crimes financiers ;
- Utilisation strictement autorisée des informations pour les besoins des missions de supervision, LAB/FT ou du renseignement financier ;
- La réciprocité des retours d'information destinée à dynamiser la transparence et la confiance mutuelle ;
- La réactivité et la célérité lors des processus des traitements des demandes d'informations ;
- L'harmonisation des politiques des autorités en matière de gestion des données et de sécurité des systèmes.

Le partage d'informations s'impose, ainsi, comme un gage d'intégrité et de sécurité du système financier et un élément fondamental du renforcement de sa résilience.

## **2. Pratique de l'échange d'informations entre les banques et les autorités réglementaires et lutte contre la criminalité financière :**

### **2.1. Etude empirique :**

#### **2.1.1 Méthodologie de recherche**

Notre recherche pratique a été matérialisée par une enquête auprès des responsables de différentes fonctions des banques et de l'Autorité Nationale du Renseignement Financier. Notre étude a été traduite



par un questionnaire, composés de 15 questions destinées à apprécier les variables d'analyse associées à chaque hypothèse de recherche retenue par nos soins.

Notre questionnaire a pour objectifs :

- L'évaluation de la perception par les responsables de la contribution de l'échange d'informations entre les banques et les autorités réglementaires à la lutte contre les crimes financiers ;
- La définition des types des données, jugées comme prioritaires pour leur partage avec les autorités réglementaires ;
- L'appréciation des éléments clés et des éléments de mesure d'efficacité de la collaboration entre les autorités réglementaires ;
- L'exploration des outils de communication exploités par les banques pour prévenir la criminalité financière.

Cinq hypothèses de recherche ont été retenues par nos soins comme suit :

→ **Hypothèse n°1** : La coordination et l'échange d'informations entre les banques et les autorités réglementaires sont importants pour assurer une lutte efficace contre les crimes financiers.

→ **Hypothèse n°2** : Les banques utilisent des normes et des protocoles de communication standardisés pour partager les informations et garantir une collaboration efficace avec les autorités réglementaires pour lutter contre les crimes financiers tels que le blanchiment des capitaux et le financement du terrorisme).

→ **Hypothèse n°3** : Les banques ont mis en place des processus de surveillance financière pour assurer la détection des transactions suspectes et le partage automatique d'informations avec les autorités réglementaires et prévenir les activités criminelles telles que le blanchiment des capitaux et le financement du terrorisme

→ **Hypothèse n°4** : Les banques collaborent avec les autorités de régulation pour échanger des données sur les activités criminelles transnationales et utilisent ces informations aux fins de leur identification et surveillance.

→ **Hypothèse n°5** : Les banques cherchent et recourent en permanence à des moyens pour améliorer la coordination avec les autorités réglementaires dans la lutte efficace contre les activités criminelles transnationales, et assurer la transparence et l'efficacité de la surveillance financière.

Notre questionnaire a donné lieu à 34 réponses dont 33 cas émanant des responsables des banques et un cas de l'ANRF.

La population consultée de 34 répondants est structurée comme suit :

- 16 analystes de la sécurité financière des banques et de l'ANRF soit 47% ;
- 9 directeurs ou responsables des agences bancaires soit 26% ;
- 4 responsables auditeurs ou contrôleurs des banques soit 12% ;
- 3 responsables de la sécurité financière des banques soit 9% ;
- 2 responsables du système d'information des banques soit 6%.

## 2.1.2. Résultats de la recherche :

### 2.1.2.1. Eléments d'appréciation de l'hypothèse numéro 1 :

#### Intitulé de l'hypothèse numéro 1 :

La coordination et l'échange d'informations entre les banques et les autorités réglementaires sont essentiels pour lutter efficacement contre la criminalité financière.

Axe de recherche N° 1 : Coordination Banques /Autorités de régulation pour la lutte contre la criminalité financière.

Cet axe consiste d'une part à établir et matérialiser le lien entre l'échange d'informations bancaires et l'efficacité de la lutte contre la criminalité financière et d'autre part, identifier les obstacles et les défis à relever pour optimiser ce partage et renforcer la coordination Banques/Autorités de régulation.

L'examen de l'hypothèse numéro 1 a été mené sur la base des trois questions suivantes :

- 1) Comment d'après vous l'échange d'informations entre les banques et les autorités réglementaires peut contribuer à la lutte contre la criminalité financière ?
- 2) Quels types d'informations estimez-vous prioritaires pour l'échange avec les autorités réglementaires en matière de lutte contre la criminalité financière ?
- 3) Selon vous, quelles sont les principales contraintes à surmonter pour optimiser la gestion des informations échangées avec les autorités réglementaires ?

Les répondants à notre questionnaire pensent majoritairement à hauteur de 79% qu'une coopération renforcée entre les banques et les autorités réglementaires permet de lutter efficacement contre la criminalité financière, alors que 76% des répondants estiment que le partage d'informations peut contribuer à une meilleure identification et détection des transactions suspectes.

### **Contribution de l'échange d'informations en matière de lutte contre la criminalité financière**

<b>Éléments de contribution</b>	<b>Nombre des réponses sur 34</b>	<b>% des répondants</b>
Coopération renforcée entre les banques et les autorités réglementaires;	27	79%
Détection et prévention des activités criminelles;	26	76%
Meilleure conformité réglementaire;	20	59%
Compréhension accrue des risques financiers;	14	41%
Renforcement de la transparence;	6	18%

Source : Nous-mêmes (2024)

Par ailleurs 78% des répondants considèrent comme prioritaires les informations échangées relatives à la nature des activités suspectes, à l'identification des clients/bénéficiaires des transactions s'agissant des informations principales aux fins de détection des mouvements de fonds illégaux.

Le manque de coordination inter-métiers et l'insuffisance des ressources allouées ont été identifiées comme principales contraintes de gestion des informations échangées respectivement par 79 % et 71% des répondants.

### **Contraintes de gestion des informations échangées avec les autorités réglementaires**

<b>Contraintes de gestion des informations échangées avec les autorités réglementaires</b>	<b>Nombre des réponses sur 34</b>	<b>% des répondants</b>
Le manque de coordination inter-métiers ;	27	79%
L'insuffisance des ressources dédiées à la gestion des échanges d'informations ;	24	71%
Réticence des remontées d'informations vers les métiers et entités opérationnelles ;	19	56%
L'absence de référentiels et des processus standardisés ;	13	38%
Difficultés à identifier avec précision certains risques atypiques.	6	18%

Source : Nous-mêmes (2024)

Les résultats de notre recherche empirique liés à ce premier volet d'analyse permettent de valider l'hypothèse 1 en montrant que la coopération renforcée par l'échange d'informations assure une meilleure lutte contre la criminalité financière.

Ces réponses ont démontré que les principaux obstacles à l'échange sont d'ordre organisationnel (coordination et ressources) plus que méthodologique ou de détection des risques, et qui impliquent la nécessité de renforcer la synergie entre métiers et l'allocation de moyens dédiés.

### **2.1.2.2. Eléments d'appréciation de l'hypothèse numéro 2 :**

#### Intitulé de l'hypothèse numéro 2 :

Les banques utilisent des normes et des protocoles de communication standardisés pour échanger des informations et garantir une coordination efficace avec les autorités réglementaires dans la lutte contre les activités criminelles telles que la fraude et le blanchiment des capitaux.

Axe de recherche N° 2 : Standardisation des échanges d'informations bancaires-autorités pour contrer la criminalité financière.

Cet axe de recherche permet de :

- Evaluer les normes actuelles d'échanges d'informations bancaires, et leur capacité à coordonner efficacement la lutte contre la criminalité financière ;
- Simplifier et optimiser les processus pour renforcer l'efficacité du partenariat Banques/Autorités sur ces sujets tout en respectant le cadre légal.

L'examen de la troisième hypothèse de notre recherche a été appréhendé à travers les questions suivantes :

- 1) Quels sont d'après vous les éléments essentiels de mesure de l'efficacité de cette coordination dans la lutte contre les activités criminelles transnationales ?
- 2) Comment, selon vous, les banques peuvent respecter les normes de communication avec les autorités réglementaires et renforcer leur efficacité en matière de prévention de la criminalité financière ?
- 3) Selon vous, dans quelle mesure la standardisation des processus de communication entre les banques et les autorités réglementaires peut-elle réduire leur charge de travail dans la lutte contre la criminalité financière ?

Sur la base des réponses recueillies, il ressort que l'examen des éléments essentiels de mesure d'efficacité et de coordination de lutte contre les activités criminelles transnationales se traduit essentiellement par la qualité et la pertinence des informations échangées à hauteur de 85% des réponses données.

Conformément à 71% des réponses obtenues, la mesure d'efficacité peut être appréciée sur la base du nombre des cas transmis au parquet pour instruction judiciaire.

Selon 88% des répondants, les banques doivent respecter les normes de communication avec les autorités réglementaires et renforcer leur efficacité en matière de prévention de la criminalité financière sur la base des actions de formation et de sensibilisation régulières de leur personnel.

La normalisation des processus de communication entre les banques et les autorités de régulation peut aider à minimiser la charge de travail dans la lutte contre la criminalité financière. Cette action peut se traduire par une communication plus efficace et rapide avec un traitement formalisé et automatisé selon 94% des répondants.

L'optimisation des processus des échanges sécurisés entre systèmes informatiques intervient en second rang avec 74% des réponses.

Ces résultats justifient l'intérêt particulier accordé par les responsables des banques aux mesures concrètes d'efficacité opérationnelle au même titre que la qualité de la coordination et les résultats concrets en justice.

Les résultats valident en grande partie l'hypothèse 2, montrant que la normalisation des échanges et le respect de normes communes par les banques permettent le renforcement de l'efficacité de la lutte contre la criminalité financière.

Les répondants estiment également que cette mesure aura davantage d'impact sur l'efficacité par le biais de la rationalisation des processus de communication opérationnels et l'automatisation des échanges.

### **2.1.2.3. Eléments d'appréciation de l'hypothèse numéro 3 :**

#### Intitulé de l'hypothèse numéro 3 :

Les banques ont mis en place des processus de surveillance financière pour assurer la détection des transactions suspectes et le partage automatique d'informations avec les autorités réglementaires et prévenir les activités criminelles telles que le blanchiment des capitaux et le financement du terrorisme

Axe de recherche N° 3 : Processus bancaires de détection et échanges d'informations avec autorités réglementaires.

Cet axe de recherche a pour objectif d'évaluer d'une part les processus de détection de transactions suspectes mis en place par les banques et identifier d'autre part les technologies pouvant faciliter ces échanges tout en respectant la protection des données.

Ceci nous permettra d'apprécier par conséquent la contribution effective des technologies à la prévention des crimes financiers.

L'analyse de la troisième hypothèse de notre recherche est effectuée sur la base des questions suivantes :

- 1) Votre établissement échange-t-il de manière automatique et sans délai des informations relatives aux transactions suspectes avec les autorités réglementaires pour permettre une action rapide ?
- 2) Quels sont selon vous les technologies pouvant être utilisées par votre établissement pour faciliter les échanges d'informations ?
- 3) Quels sont les outils utilisés par votre établissement en matière d'échange des informations avec les banques et avec les autorités réglementaires ?

La consolidation des réponses liées à cette hypothèse a dégagé les résultats suivants :

S'agissant des modalités d'automatisation des échanges entre les banques et les autorités, la majorité des répondants estime que le partage d'informations est soumis en général à une validation préalable.

Conformément aux réponses obtenues, l'échange des informations entre les banques et les autorités réglementaires est assuré via par une plateforme dédiée spécialement à la déclaration des soupçons de la clientèle et à l'émission des demandes et production des informations en rapport avec la connaissance des clients et leurs transactions.

L'échange des informations avec l'ANRF est assuré par le correspondant habilité de la banque auprès de cet organisme.

Par ailleurs, les principales technologies pouvant être utilisées par les banques pour faciliter les échanges d'informations sont récapitulées comme suit :

- Les plates-formes digitales collaboratives sécurisées selon 68% des répondants ;
- L'intelligence artificielle pour automatiser les analyses selon 65% des avis recueillis ;
- Le cloud computing pour le stockage et le partage sécurisé des données conformément aux réponses de 59% des personnes sondées.

Ces données indiquent que les banques se basent avant tout sur des outils opérationnels de gestion des flux financiers ainsi que sur des standards de communication et des interlocuteurs privilégiés.

Les résultats du questionnaire valident en partie l'hypothèse 3 en soulignant le recours à des plateformes dédiées, même si l'automatisation complète des échanges semble encore perfectible selon les banques interrogées.

### **2.1.2.4. Eléments d'appréciation de l'hypothèse numéro 4 :**

#### Intitulé de l'hypothèse numéro 4 :

Les banques collaborent avec les autorités réglementaires pour échanger des informations sur les activités criminelles transnationales et utilisent ces informations pour identifier et surveiller les activités criminelles.

Axe de recherche N° 4 : Collaboration Banques/Autorités réglementaires contre la criminalité transnationale.

Cet axe de recherche porte sur :

- L'analyse de l'organisation interne des processus bancaires d'échange d'informations avec les autorités de régulation ;
- L'identification des obstacles réglementaires et opérationnels en matière du partage des données et les modalités du renforcement de leur efficacité, confidentialité et sécurité.

L'analyse de cette hypothèse a été effectuée sur la base des trois questions suivantes :

- 1) Comment votre établissement organise en interne le processus d'échange d'informations avec les autorités réglementaires pour lutter contre les activités criminelles ?
- 2) Quels sont selon vous, les obstacles réglementaires et opérationnels d'un partage efficace d'informations entre les banques et l'ANRF ?
- 3) Comment votre établissement assure-t-il la sécurité et la confidentialité des informations échangées avec les autorités réglementaires ?

La consolidation des réponses aux questions associées à cette hypothèse a dégagé les résultats suivants : Selon plus de 85% des répondants, le processus d'échange d'informations avec les autorités réglementaires pour lutter contre les activités criminelles est organisé par :

- La mise en place d'une unité dédiée au traitement des alertes et à la liaison avec les autorités ;
- L'instauration des procédures claires de validation/transfert des signalements vers les interlocuteurs externes.

La coordination rapprochée entre équipes de détection interne et services de conformité intervient pour 59% des cas.

Les répondants accordent une priorité aux aspects opérationnels concrets assurant des échanges d'informations efficaces.

Les principaux obstacles réglementaires et opérationnels identifiés par les répondants pour un partage efficace d'informations portent sur les :

- Contraintes de la réglementation au détriment de l'efficacité opérationnelle (71%) ;
- Freins opérationnels liés aux volumes des données et aux délais du traitement des informations (68%).

S'agissant de la sécurité et la confidentialité des informations échangées avec les autorités de régulation, elle est assurée par l'élaboration et la mise en œuvre des politiques de gestion et de limitation des accès aux informations sensibles selon 85% des réponses et par la supervision de la confidentialité et la sécurité des informations partagées (68% des cas).

Les résultats valident partiellement l'hypothèse 4 en montrant que les banques ont organisé des processus d'échange avec les autorités, mais que des obstacles réglementaires et opérationnels subsistent.

A cet égard, ils précisent que la sécurité et la confidentialité des échanges sont assurées via des politiques de gestion appropriées. Cependant, des améliorations sont encore nécessaires, notamment sur les aspects opérationnels et de sécurisation des données échangées.

#### **2.1.2.5. Eléments d'appréciation de l'hypothèse numéro 5 :**

Intitulé de l'hypothèse numéro 5 :

Les banques cherchent constamment, des moyens d'améliorer la coordination avec les autorités réglementaires nationales et internationales dans la lutte efficace contre les activités criminelles transnationales, et assurer la transparence et l'efficacité de la surveillance financière.

**Axe de recherche N° 5 :** Amélioration de la coordination Banques/Autorités réglementaires en matière de lutte contre la criminalité transnationale.

Cet axe a pour objectif de proposer des pistes concrètes pour le renforcement de l'efficacité de la surveillance financière dans la lutte contre les crimes transnationaux à travers :

- L'identification des leviers d'automatisation prioritaires pour améliorer la coordination bancaire avec les autorités réglementaires ;
- La définition des conditions clés d'une coopération efficace et les défis liés aux échanges internationaux d'informations.

La cinquième hypothèse de notre recherche a fait l'objet d'une analyse au travers des questions suivantes :

- 1) Quels sont les processus jugés prioritaires à automatiser pour améliorer la coordination de la banque avec les autorités réglementaires ?
- 2) Quelles sont selon vous les conditions clés pour une coopération efficace entre les banques et les autorités réglementaires dans la lutte contre la criminalité financière ?
- 3) Quels sont les défis auxquels les banques sont confrontées lorsqu'elles échangent des informations avec des acteurs ou entités à l'étranger (succursales, filiales etc..) ?

Les résultats des réponses aux questions liées à la cinquième hypothèse de notre recherche sont synthétisés comme suit :

Selon 85% des réponses, les processus jugés prioritaires à automatiser pour améliorer la coordination de la banque avec les autorités de régulation portent sur la surveillance et la détection de transactions suspectes.

Le traitement, le partage et le signalement immédiat des alertes aux autorités réglementaires sont jugés privilégiés respectivement par 79% des répondants.

Ces résultats démontrent que les établissements bancaires privilégient l'automatisation des processus opérationnels clés comme la détection et le partage d'informations sensibles, plutôt que des tâches d'une valeur ajoutée assez moindre tels que l'analyse des risques transfrontaliers.

Les conditions clés pour une coopération efficace entre les banques et les autorités réglementaires dans la lutte contre la criminalité financière ont été traduites par les résultats suivants :

#### **Conditions de coopération dans la lutte contre la criminalité financière :**

<b>Conditions d'efficacité de coopération dans la lutte contre la criminalité financière</b>	<b>Nombre de réponses sur 34</b>	<b>% des répondants</b>
Cadre juridique commun et partage de données sécurisé ;	28	<b>82%</b>
Confidentialité et responsabilité clarifiées dans les échanges ;	26	<b>76%</b>
Coordination opérationnelle et Interopérabilité des outils de détection et d'analyse ;	21	<b>62%</b>
Evaluation régulière de la performance du dispositif ;	15	<b>44%</b>
Veille commune sur l'évolution des risques émergents.	12	<b>35%</b>

**Source : Nous-mêmes (2024)**

Les banques peuvent être confrontées à plusieurs défis lors de l'échange des informations avec des acteurs ou entités à l'étranger (succursales, filiales etc.), dont principalement :

- La diversité et complexité de réglementation et de normes citées par 74% des répondants ;
- Le maintien de la conformité face à l'évolution permanente de la réglementation ayant obtenu 71% des réponses.

En somme, les défis principaux sont liés à la complexité réglementaire internationale et à la permanence du suivi de l'évolution du cadre normatif.

L'hypothèse n°5 est globalement validée par les réponses qui confirment la volonté des banques d'améliorer la coordination avec les autorités notamment via l'automatisation des processus clés de détection et de partage d'informations. Néanmoins, des efforts restent à faire sur certains aspects comme l'analyse des risques transfrontaliers.

#### **2.1.2.6. Synthèse des résultats du questionnaire :**

En somme, on peut déduire les principaux résultats suivants :

- L'efficacité des échanges d'informations sur les activités criminelles reste tributaire d'une meilleure coordination et collaboration entre les banques et les autorités de régulation ;
- L'utilisation de technologies de pointe à l'instar d l'intelligence artificielle et le cloud computing facilite le partage rapide et sécurisé des informations entre les acteurs concernés ;
- L'harmonisation des réglementations nationales et internationales sur le partage d'informations financières facilite la coopération transfrontalière dans la lutte contre la criminalité financière ;
- L'efficacité des échanges d'informations est renforcée également par la formation et la sensibilisation accrues du personnel bancaire sur les procédures de détection et de signalement des activités criminelles ;
- Les processus automatisés mis en place par les banques leur permettent d'assurer un partage rapide des alertes des transactions suspectes et leur signalement aux autorités de régulation en temps opportun.

#### **2.2 Collaboration Banques / Autorités de régulation et lutte contre la criminalité financière :**

L'implication des banques dans les crimes financiers a pour effet d'impacter leur sécurité financière et réputation (European Banking Authority : Décembre 2021).

Pour cette raison, la lutte contre le crime financier constitue une préoccupation majeure de la gouvernance bancaire.

Les banques ont longtemps eu du mal à détecter les cas des fraudes et du blanchiment des capitaux en raison du nombre élevé de transactions à surveiller quotidiennement.

Néanmoins, des plateformes de partage d'informations entre les banques et les autorités réglementaires se développent pour améliorer les processus de leur détection.

Les diverses études de recherche et la mise en œuvre des normes et réglementation internationales ont mis en évidence le rôle déterminant des banques en matière de détection et de prévention de la criminalité financière.

En plus d'une identification précise des clients et de l'examen de leurs transactions, l'action concertée des banques permet de mieux déclarer et communiquer les flux financiers illicites aux autorités réglementaires. D'où l'importance d'une coopération étroite et renforcée entre les banques et les autorités qui s'impose pour faire face à cette catégorie des risques.

La coordination en matière d'échange d'informations inter banques et avec les autorités de régulation s'avère déterminante et complémentaire pour rendre plus efficace la maîtrise des risques des crimes auxquels le secteur financier est confronté.

Le partage des données et l'exploitation des dispositifs dédiés doit avoir pour objectif de favoriser la détection et une réaction renforcée face à la criminalité financière.

Les plateformes du partage d'informations sont censées également encourager le développement des approches concertées en termes de gestion des risques et du contrôle interne bancaire et pouvoir produire en conséquence des réponses aux incidents par les banques.

La coordination et l'engagement des autorités restent tributaires d'un partage sécurisé des données et de la mise en œuvre des protocoles d'échange performants pour contrecarrer de manière efficace les réseaux financiers illicites.

Selon une étude réalisée par l'ACPR France en Juin 2023, les banques et les autorités de régulation se partagent des responsabilités importantes en la matière.

A cet effet les banques sont tenues de :

- Assurer la collecte et l'analyse des informations sur la clientèle ;
- Effectuer une identification de leur clientèle de manière approfondie et la surveillance rigoureuse de leurs transactions ;
- Assurer l'échange des informations et le signalement des transactions suspectes aux autorités compétentes.

Les banques sont également responsables de l'identification des vulnérabilités associées aux activités de la clientèle et des modalités d'analyse des risques du blanchiment de capitaux et de financement du terrorisme

D'autre part les autorités réglementaires supervisent les activités des banques et s'assurent de la bonne application de la réglementation en vigueur.

Leur mission principale consiste à effectuer toutes les investigations nécessaires à l'effet de vérifier la conformité des banques, diligenter des mesures disciplinaires à l'encontre des établissements défailants et sanctionner les manquements constatés.

Les cellules de renseignement financier (CRF) jouent un rôle déterminant en matière d'analyse et du partage d'informations objet des transactions inhabituelles/suspectes, et s'imposent comme intermédiaires entre le secteur privé et les autorités répressives (FATF : 2021).

### **2.2.1 Gouvernance et organisation de l'échange des informations :**

Conformément à une étude élaborée par Quinte, T en 2022, le rôle central de la gouvernance consiste à organiser et encadrer de manière solide les échanges entre les banques et les autorités de régulation. Leur mission se traduit par :

- La mise en place des politiques et la définition des procédures et des conditions d'échange d'informations, conformément au cadre réglementaire ;
- L'élaboration des mécanismes de collaboration efficaces dont des canaux de communication sécurisés entre les banques et les autorités réglementaires ;
- Le respect de la conformité permanente des banques à la réglementation d'échange de données ;
- La gestion et la maîtrise des risques associés à la protection de la clientèle et à la confidentialité de leurs données ;
- La supervision du fonctionnement efficace et transparent des processus d'échange des données.

Le bon fonctionnement et le suivi des plateformes d'échange d'informations requièrent une gouvernance robuste et responsable compte tenu de leur importance et rôle stratégique.

Le niveau d'implication de la gouvernance reste tributaire d'une gestion optimale des risques, et de la responsabilité juridique des acteurs de référence.

En tant que bases précieuses d'informations, les plateformes d'échange sont exposées à des tentatives d'attaques qui nécessitent une amélioration des normes et des processus de sécurité des données.

Le partage des données, les expertises et le retour d'expérience au sein de plateformes communes faciliterait une riposte consolidée face aux infractions financières.

Cette démarche permet de consolider les approches de gestion et dynamiser la maîtrise des risques.

### **2.2.2. Défis et perspectives de recherche sur l'échange des informations et développement de nouvelles technologies :**

L'échange d'informations fait face à des défis multiples portant sur :

- La sécurité et le respect de la confidentialité des données ;
- La compatibilité et l'inter connectivité des systèmes hétérogènes ;
- Le volume croissant des informations issues de la numérisation requérant d'outils d'analyses solides ;
- Les besoins d'informations en temps réel devant permettre la détection précoce des activités suspectes ;
- L'évolution des exigences réglementaires ;
- L'évolution technologique et l'avènement entre autres de la cryptographie, et le traitement de données massives.



Dans ce contexte, les défis actuels peuvent ainsi être dépassés grâce aux avancées technologiques. Celles-ci sont censées assurer un partage d'informations plus sûr, fluide et automatisé entre systèmes interopérables et optimiser en conséquence leur efficacité et leur sécurité.

### **2.3. Perspectives de recherche sur l'échange des informations et développement des nouvelles technologies :**

De recherches futures pourraient être axées sur le développement de techniques avancées garantissant la confidentialité et la protection des données échangées.

Elles pourraient explorer des méthodes pour renforcer l'intégration et l'interopérabilité des systèmes hétérogènes des banques et des autorités réglementaires.

L'utilisation des nouvelles technologies (notamment l'intelligence artificielle, du machine Learning et blockchain) représentent des voies prometteuses de recherches notamment en matière d'analyse des données financières, l'amélioration de la transparence et la sécurité des informations échangées.

Une attention peut être allouée aux incidences de l'évolution de la réglementation sur les pratiques, les innovations et les avancées technologiques. Ce qui a pour effet de d'assurer une supervision plus renforcée des activités bancaires.

### **2.4 Mesures et propositions d'amélioration de l'échange d'informations entre les banques et les autorités réglementaires en matière de lutte contre la criminalité financière :**

Le secteur public doit jouer un rôle important afin de faciliter les actions du partage d'informations du secteur privé. Il pourrait diriger des projets pilotes pour permettre aux institutions financières d'explorer le partage de données de manière encadrée et réglementée. (Maxwell, N (2022).

La législation et la réglementation devraient être mises à jour si nécessaire pour clarifier le cadre applicable au partage d'informations privées.

Dans cette optique, le GAFI a préconisé la conception des stratégies nationales de partage d'informations qui aligne les projets du secteur privé sur les priorités publiques.

Ces actions visent à :

- Développer une interaction constructive avec les autorités de régulation ;
- Tirer parti du potentiel des nouvelles technologies afin d'optimiser la fiabilité l'efficacité, et la sécurité des échanges ;
- Mettre en place des mécanismes de sécurité, du contrôle et de suivi de l'usage des informations échangées y compris des vérifications indépendantes et le signalement confidentiel des soupçons ;
- Déployer des mécanismes formels et informels d'échange d'informations, et notamment par le biais des plateformes collaboratives.

Ces stratégies doivent apporter une contribution proactive aux objectifs de lutte contre la criminalité financière, préserver l'intégrité des échanges.

### **Conclusion générale :**

L'échange d'informations entre les banques et les autorités réglementaires favorise une compréhension réciproque des risques et une concertation mutuelle pour contrer les menaces émergentes.

Le partage de données et des pratiques a pour effet de consolider les aptitudes d'identification et de maîtrise des vulnérabilités liées aux infractions financières.

Il est cependant essentiel d'assurer un équilibre entre les échanges nécessaires requis et la sauvegarde des informations à caractère sensible et confidentiel.

Les progrès technologiques sont conçus pour promouvoir et optimiser la coopération.

A cet effet les perspectives de recherche dans ce domaine peuvent être axées sur le développement de la résilience du secteur financier.

Selon le GAFI, l'efficacité des systèmes de lutte contre le blanchiment des capitaux et le financement du terrorisme dépend d'un partage continu et sécurisé des données et d'une coordination étroite banque/autorités publiques.

Toutefois, les exigences du respect de la réglementation sur la protection des données personnelles peuvent entraver ces échanges sur le plan juridique.

Par conséquent les parties en cause doivent forger des réponses opérationnelles dans le but de concilier ces impératifs face à l'évolution des menaces de la criminalité financière et au développement des nouvelles technologies.

En somme, le partage d'informations avec les autorités de régulation constitue un appui incontournable pour faire face à la criminalité financière au niveau du secteur bancaire et préserver sa résilience et son intégrité.

### **Bibliographie :**

Comité de Bale. (2002). Partage des dossiers financiers entre juridictions dans le cadre de la lutte contre le financement du terrorisme. Bank Of International Settlement.

Crédit Suisse (2018) Automatic Exchange of Information (AEI) Glossary

Fédération Bancaire Française (2009) La lutte contre le blanchiment de capitaux et le financement du terrorisme Clés de la banque.

European Banking Authority (2021) Guidelines on cooperation and information exchange between prudential supervisors, AML/CFT supervisors and financial intelligence units under directive 2013/36.

FATF (2012). Recommandations du GAFI Normes internationales sur la lutte contre le blanchiment de capitaux et le financement du terrorisme et de la prolifération, mise à jour Mars 2022, GAFI .Paris . France.

FATF (2022), Partnering in the Fight Against Financial Crime: Data Protection, Technology and Private Sector Information Sharing, FATF .Paris . France.

FATF (2021), Stocktake on Data Pooling, Collaborative Analytics and Data Protection, FATF.Paris. France.

FATF (2018), Professional Money Laundering, FATF. Paris. France.

FATF (2013-2021), Méthodologie d'évaluation de la conformité technique aux Recommandations du GAFI et de l'efficacité des systèmes de LBC/FT, mise à jour Octobre 2021, GAFI .Paris . France.

FATF (2017), Orientations sur le partage d'informations avec le secteur privé, GAFI. Paris. France.

Maxwell, N (2022). A Survey and Policy Discussion Paper: 'Lessons in private financial information sharing to detect and disrupt crime'. Future of Financial Intelligence Sharing (FFIS) research programme.

Monetary Authority of Singapore (2023) FI-FI (Financial Institution) Information-Sharing Platform for AML/CFT .Consultation paper on FI-FI information sharing platform for AML/CFT.

Quintel, Teresa (2022) Data protection rules applicable to Financial Intelligence Units: still no clarity in sight ERA Forum Journal of the Academy of European Law Germany.

Tambunan, M(2020) The implementation of exchange of information in the banking industry Vol 22 No 2 (2020): Jurnal Bisnis dan Akuntansi Indonesia.