LE DÉFI DE LA PROTECTION DES DONNÉES PERSONNELLES FACE AUX EXIGENCES LÉGALES ET RÈGLEMENTAIRES (LCB/FT, LUTTE CONTRE LA FRAUDE)

22èmes JOURNEES DE L'ASSOCIATION AFRICAINE DES JURISTES DE BANQUES ET ETABMISEMENTS FINANCIERS D'AFRIQUE (**AJBEF**)

24-27 Nov. 2025, OUAGA, SOPATEL SILMANDE

Dr Ibrahim COULIBALY

Expert en droit du numérique, Consultant

Cabinet JurisNumeris SARL

cab.jurisnumeris@gmail.com

INTRODUCTION

Les données de l'équation :

- Les institutions financières sont soumises à des obligations de lutte contre le blanchiment de capitaux et le financement du terrorisme.
- Le respect de ces obligations implique un traitement de données à caractère personnel dont la mise en œuvre oblige les institutions financières à adopter des mesures pouvant être attentatoires aux droits des personnes

Exemple : Arrêt de la Cour de justice de l'Union européenne (CJUE) du 22 novembre 2022 dans les affaires jointes C-37/20 Luxembourg Businesses Registers et C-601/20 Sovim

- **LCB/FT et PDCP : entre obligation de surveillance/transparence et obligation de protection des personnes : quels équilibres ?**

PLAN

I – Les obligations de lutte contre le blanchiment de capitaux et financement du terrorisme des institutions financières

II – Les obligations de protection des données à caractère personnel pesant sur les institutions financières

III – Recommandations

IV – Conclusion

I – Les obligations de lutte contre le blanchiment de capitaux et financement du terrorisme des institutions financières

- **Existence d'une législation foisonnante**

- au niveau international,
- régional
- sous-régional
- national

- **Existence d'organismes de contrôle (GAFI, CENTIF)**


GAFI
NORMES INTERNATIONALES SUR LA LUTTE CONTRE LE BLANCHIMENT DE CAPITAUX ET LE FINANCEMENT DU TERRORISME ET DE LA PROLIFÉRATION
Les Recommandations du GAFI
Mise à jour juin 2025

Au niveau africain

- **Directive** n° 02/2015/cm/UEMOA relative à la lutte contre le blanchiment de capitaux et le financement du terrorisme dans les Etats membres de l'Union économique et monétaire ouest africaine (UEMOA)
- **Loi uniforme** relative à la lutte contre le blanchiment de capitaux, le financement du terrorisme et de la prolifération des armes de destruction massive dans les Etats membres de l'UMOA ;
- **Instruction** n°003-03-2025 du 18 mars 2025 relative à l'identification, la vérification de l'identité et la connaissance de la clientèle par les institutions financières
- **Instruction** n°001-03-2025 du 18 mars 2025 portant modalités de mise en œuvre par les institutions financières de leurs obligations en matière d'organisation, de contrôle interne et de conformité aux exigences de lutte contre le blanchiment des capitaux
- **Instruction** n° 007-09-2017 portant modalités d'application par les institutions financières de la loi uniforme relative a la lutte contre le blanchiment de capitaux et le financement du terrorisme dans les Etats membres de l'UMOA

Quelques obligations de LCB/FT à la charge des institutions financières

- Adoption de procédures internes de prévention (Instruction n° 007-09-2017)

Les procédures prescrivent les diligences à accomplir et les règles à respecter en matière :

1. d'identification et de connaissance de la clientèle ;

2. de constitution et d'actualisation des dossiers de la clientèle ;

3. de fixation de délais pour la vérification de l'identité des clients et la mise à jour des informations y afférentes ;

4. d'identification et de suivi des opérations concernant des personnes politiquement

exposées aux risques de blanchiment de capitaux et de financement du terrorisme ;

5. d'élaboration d'une cartographie et d'évaluation des risques de blanchiment de capitaux et de financement du terrorisme auxquels l'institution financière est exposée ;

- **La collecte de données personnelles** (Instruction n°003-03-2025)

« L'institution financière identifie son client personne physique, en collectant les informations ci-après :

- les nom et prénoms ;
- les date et lieu de naissance ;
- la nationalité ;
- l'adresse du domicile ;
- le numéro de la pièce d'identification ».

Ces données doivent être vérifiées, authentifiées

- **La mise en place d'un système d'information** (Instruction n°001-03-2025 du 18 mars 2025)

L'institution financière se dote d'un système d'information permettant, notamment :

1. le profilage des clients et des comptes ouverts dans ses livres ;
2. le filtrage en temps réel des clients et des transactions ;
3. le suivi des mouvements sur les comptes et la génération des alertes ;
4. la détermination du solde global de l'ensemble des comptes détenus par un même client ;
S. le recensement des opérations effectuées par un même client, qu'il soit occasionnel ou habituel ;
6. l'identification des transactions à caractère suspect ou inhabituel.

L'institution financière prend en compte toute information de nature à modifier le profil du client et l'intègre au système d'information dans un délai maximum d'un mois.

Le système d'information doit également assurer que les modifications relatives à la mise en œuvre des sanctions financières ciblées sont prises en compte sans délai, conformément aux dispositions de l'article 89 de la Loi uniforme relative à la LBC/FT/FP.

L'efficacité du système d'information doit faire l'objet d'un examen périodique, au moins une fois par an, en vue d'adapter ledit système à la nature et à l'évolution de l'activité de l'institution financière ainsi que de l'environnement légal et réglementaire.

La mise en œuvre des obligations ci-dessus citées :

- Est constitutive d'un traitement de données à caractère personnel
- Soumise à la loi relative à la protection des données à caractère personnel
- A laquelle les institutions financières doivent se conformer

II – Les obligations de protection des données à caractère personnel pesant sur les institutions financières

*** Existence d'une législation foisonnante au niveau**

- international,
- régional,
- sous-régional
- national

- **Existence d'autorités de protection des données** (CIL, CPD, etc.)

Quelques textes de référence

- Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (dite Convention 108)
- Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel
- Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (**Règlement Général sur la Protection des Données**)
- Acte additionnel A/SA.1/10/10 relatif à la protection des données à caractère personnel dans l'espace de la CEDEAO
- Convention de l'Union africaine sur la cybersécurité et la protection des données à caractère personnel (dite Convention de Malabo), 2014

Quelques notions de base

- Notion de données à caractère personnel

« **toute information** de quelque nature qu'elle soit et indépendamment de son support, y compris le son et l'image **relative à une personne physique identifiée ou identifiable, directement ou indirectement**, par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique ».

- Notion de traitement de données

« **toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés, et appliquées à des données**, telles que la collecte, l'exploitation, l'enregistrement, l'organisation, la conservation, l'adaptation, la modification, l'extraction, la sauvegarde, la copie, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, le cryptage, l'effacement ou la destruction de données à caractère personnel ».

- Responsable de traitement, sous-traitant, fichier, personne concernée, destinataires

Champ d'application de loi

« sont soumis aux dispositions de la présente loi :

- toute collecte, tout traitement, toute transmission, tout stockage et toute utilisation des données à caractère personnel par une personne physique, l'Etat, les collectivités locales, les personnes morales de droit public ou de droit privé ;

- tout traitement automatisé ou non automatisé de données contenues ou appelées à figurer dans un fichier ;

- *tout traitement de données mis en œuvre sur le territoire national ;*
- tout traitement de données concernant la sécurité publique, la défense, la recherche et la poursuite d'infractions pénales ou la sûreté de l'Etat, sous réserve des dérogations définies par des dispositions spécifiques fixées par d'autres textes de lois en vigueur ».

Les institutions financières sont donc soumises aux lois relatives à la protection des données personnelles

- **De la protection des données personnelles en pratique / mise en conformité avec la loi**

- Ensemble de règles de fond et de forme

- Principes de base de protection des données personnelles

- **Principe de finalité** (finalité initiale et réutilisation)

Légitimité de principe (Loi LCB/FT)

Réutilisation compatible (utilisation d'une Déclaration d'Opération Suspecte « DOS » par les organismes de contrôle aux de fins de poursuites)

Alerte : détournement de finalité !

- **Principe de licéité**

- **Accomplissement des formalités préalables requises** : autorisation, déclaration, avis

Attention aux fichiers clandestins !!!!!!!

- **Information et recueil du consentement des personnes concernées**

Une information précise [.....] claire et compréhensible

Problématique de la limitation de l'information (déclaration de transactions suspectes)

Un traitement de donnée reposant en principe sur le consentement des personnes

Exceptions au recueil du consentement (obligation légale pesant sur le responsable du traitement, exécution d'une mission de service public, mise en œuvre d'obligations contractuelles, sauvegarde des intérêts vitaux)

- **Principe de proportionnalité des données**

Toutes les données collectées doivent être adéquates, pertinentes et non excessives.

Le traitement des données doit être limité à ce qui est nécessaire pour atteindre une finalité légitime et prédéterminée.

En pratique, le traitement d'une plus grande quantité de données à caractère personnel, y compris la vérification de ces données à partir de diverses sources accessibles à l'entité assujettie, peut être nécessaire.

Enjeu : justification de la pertinence des données au regard de la finalité.

*** Principe d'exactitude des données**

« Les données collectées doivent être exactes et, si nécessaire, mise à jour ».

Les implications de ce principe sont nombreuses en incluant notamment la validation des procédés de collecte des données ou la qualification professionnelle des personnes procédant à la collecte.

Instruction n°003-03-2025 du 18 mars 2025

Article 26 : Pondération des facteurs de risques

« Lorsqu'elle pondère les facteurs de risques dans le cadre de la classification mentionnée à l'article 25 ci-dessus, l'institution financière veille à ce que les pondérations :

1. ne soient pas influencées de manière excessive par un seul facteur ;

2. ne soient pas influencées par des considérations d'ordre économique ou de profit ;

3. ne créent pas une situation dans laquelle il est impossible de classer une relation d'affaires ou une transaction comme présentant un risque élevé ».

*** Principe d'exactitude des données**

Si les entités assujetties utilisent des systèmes automatisés, y compris gérés par un traitement algorithmique ou l'intelligence artificielle pour le profilage du risque des clients ou des bénéficiaires effectifs, **des mesures appropriées doivent être prises pour corriger les facteurs d'inexactitude des données et limiter les risques d'erreurs inhérents au profilage.**

Principe de limitation de la durée de conservation

Les données à caractère personnel ne peuvent être conservées au-delà de la durée nécessaire à la réalisation de la finalité du traitement.

Implication de principe : les données à caractère personnel doivent être effacées ou rendues anonymes dès qu'elles ne sont plus nécessaires pour les finalités pour lesquelles elles ont été collectées.

Existence de délais légaux en matière bancaire : 10 ans après la clôture du compte

Exception : possible conservation des données au-delà la réalisation de la finalité dans des cas justifiés, en vertu d'une disposition législative

Principe de sécurité des données

« Le responsable du traitement est tenu de prendre toute précaution au regard de la nature des données et, notamment, pour empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès ».

Lorsque le traitement est mis en œuvre pour le compte du responsable du traitement, celui-ci choisit un sous-traitant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements effectuer.

Il incombe au responsable du traitement ainsi qu'au sous-traitant de veiller au respect de ces mesures ».

Le respect du principe de sécurité des données nécessite des mesures techniques et organisationnelles telles que le chiffrement (fort et de bout en bout) des données et des règles de traçabilité complète des échanges, notamment par la mise en place de journaux d'accès.

Le respect des droits des personnes concernées par les données

- droit à l'information
- droit d'accès aux données à caractère personnel
- droit de rectification des données
- droit d'opposition
- droit d'effacement des données
- droit à l'oubli numérique
- droit à la portabilité des données
- ***droit de ne faire l'objet d'une décision basée sur un profilage automatisé***

- ***droit de ne faire l'objet d'une décision individuelle automatisée (DIA)***

« aucune décision administrative ou privée impliquant une appréciation sur un comportement humain ne peut avoir pour seul fondement un traitement automatisé de données à caractère personnel donnant une définition du profil ou de la personnalité de l'intéressé ».

DIA/Profilage/SCORING

Le profilage est l'analyse prévisionnelle du comportement d'une personne qui effectuée sur la base d'un traitement automatisé de données à caractère personnel donnant une définition du profil ou de la personnalité de cette personne.

C.J.U.E., 7 décembre 2023, SCHUFA Holding (Scoring), aff. C-634/21

Une telle décision est interdite sauf si elle repose sur l'un des fondements énumérés par ce texte, à savoir : la nécessité à la conclusion ou à l'exécution d'un contrat, le consentement explicite de la personne concernée, ou une autorisation législative spécifique.

Lignes directrices sur la protection des données pour le traitement des données à caractère personnel à des fins de lutte contre le blanchiment de capitaux et le financement du terrorisme

Comité de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel

Règles et principes de protection des données

Convention 108

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

CONCLUSION

Au-delà du défi, l'opportunité

La loi sur la protection des données n'est pas une loi qui interdit les traitements de données, c'est une législation d'équilibre entre l'intérêt légitime du responsable de traitement des données et le respect des droits des personnes.

Le défi de l'application sectorielle d'une loi généraliste.