LE LIVRE BLANC

LES LOGICIELS DE FILTRAGE « NAME SCREENING »

LES BONNES PRATIQUES DANS LE DOMAINE DE LA SÉCURITÉ FINANCIÈRE (SANCTIONS INTERNATIONALES, PERSONNES POLITIQUEMENT EXPOSÉES, LUTTE CONTRE LA CORRUPTION)

CE LIVRE BLANC A ÉTÉ RÉDIGÉ PAR BeCLM

Sommaire

Introduction

Le « Name Screening » : un outil central dans la lutte contre la criminalité financière

La criminalité financière est une menace persistante et en constante évolution qui affecte des institutions à l'échelle mondiale. Elle englobe diverses activités illégales, dont le blanchiment d'argent, le financement du terrorisme et la fraude financière.

Dans ce contexte complexe et en mutation, le « name screening » s'impose comme la solution cruciale pour identifier et prévenir les activités illicites. Ce processus implique le filtrage des noms de personnes et d'entités avec des listes de surveillance et des bases de données pour détecter les risques potentiels de criminalité financière.

Explorer et comparer les outils de criblage

Ce livre blanc vise à explorer les solutions logicielles de « name screening », en mettant l'accent sur leur rôle dans la prévention et la détection de la criminalité financière. Nous examinerons les technologies sous-jacentes, les défis liés à leur mise en œuvre et les meilleures pratiques pour maximiser leur efficacité. En outre, ce document s'adresse aux professionnels et à toute partie prenante intéressée par la compréhension et l'optimisation des outils de « name screening ».

Le « Name Screening » est essentiel à plus d'un titre

Le « name screening » n'est pas seulement une exigence réglementaire comme le souligne l'ACPR dans ses lignes directrices ; c'est une nécessité opérationnelle dans le paysage actuel de la criminalité financière.

Avec l'augmentation du volume des transactions et la sophistication croissante des réseaux criminels, les entreprises assujetties à la réglementation de lutte contre le blanchiment doivent être équipées pour identifier rapidement et avec précision les alertes sur les personnes à risques.

Les solutions logicielles de «name screening» jouent un rôle clé dans cette démarche, en permettant un filtrage efficace et en temps réel des relations d'affaires (clients, payeurs, prospects, fournisseurs, ...) et même des salariés[1].

Comment est structuré ce Livre Blanc

Ce livre blanc se structure autour de plusieurs chapitres clés, chacun abordant un aspect différent des solutions logicielles de «name screening».

Nous débuterons par une vue d'ensemble de la criminalité financière, suivie d'une analyse approfondie des technologies impliquées dans le «name screening».

Après un développement sur le traitement de filtrage dont la bonne compréhension est nécessaire lorsqu'on souhaite s'équiper d'une solution de « name screening », nous aborderons ensuite les fonctionnalités et les cas d'utilisation critiques qui permettent de discriminer les différentes solutions en regard des besoins propres de chaque entreprise.

Enfin nous illustrerons les bonnes pratiques de « name screening » à travers différentes études de cas.

En offrant une compréhension globale des solutions logicielles de «name screening» et de leur importance dans la lutte contre la criminalité financière, ce livre blanc vise à équiper les lecteurs des connaissances et des outils nécessaires pour naviguer efficacement dans ce domaine complexe et en constante évolution.

[1] *Exigence visée dans le code monétaire et financier*

CHAPITRE 1

NAME SCREENING : L'ÉTUDE HEC

Comme chaque année, nous demandons à notre partenaire HEC Junior de sonder les utilisateurs des solutions de « name screening ».

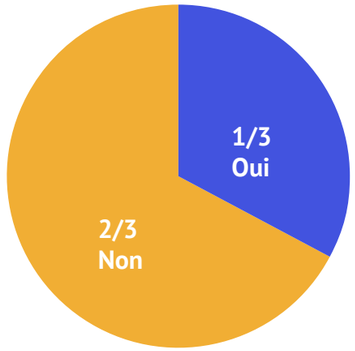
Le nouveau bâtiment du MBA d'HEC a été conçu par l'architecte David Chipperfield, lauréat du prix Pritzker en 2023.

Les points saillants de l'étude 2022

En 2022, nous avions sondé les utilisateurs sur les services associés aux solutions de filtrage. Pour rappel les points saillants de cette étude étaient :

- Malgré le poids du temps passé au traitement des faux positifs et le manque de valeur ajoutée de cette activité, 2/3 des sondés ne souhaitaient pas utiliser un prestataire pour traiter les faux positifs :

Envisagez-vous d'utiliser un prestataire pour vous aider dans le filtrage de vos relations d'affaires ?



- Les attentes très fortes sur l'accompagnement métier et cela dans les secteurs à plus forte maturité réglementaire :

Quels sont les catalyseurs au changement lors du choix d'un solution de screening ?

	Banques	Organismes d'assurance	Fintech
Un accompagnement métier et pas seulement technique	73%	63%	14%
Une technologie plus poussée	73%	75%	86%
Une offre concurrentielle et transparente	55%	38%	29%
Une interface plus ergonomique	45%	75%	29%

NAME SCREENING : L'ÉTUDE HEC

Ce qu'il faut retenir de l'étude 2023

4 points retiennent particulièrement l'attention :

1 - Les fréquences de filtrages restent encore relativement éloignées des attendus réglementaires

A. 22% des sondés ne filtrent pas quotidiennement leurs opérations
B. Pour le filtrage du portefeuille, 32% de l'échantillon n'opère pas de filtrage quotidien.
C. Sur les raisons évoquées par les sondés qui n'opèrent pas un filtrage quotidien, 3 causes principales : le coût, les limites techniques des logiciels, et les difficultés d'extraction des données.

2 - Les méthodes d'évaluation des similarités sont une boîte « noire » pour beaucoup d'utilisateurs

A. Plus de 40% des sondés ne connaissent pas le mode de fonctionnement de leurs algorithmes de filtrage.
B. Un traitement efficace des alertes nécessitant une connaissance approfondie de ses modes de fonctionnement, nous relevons ici les risques associés à la mise en place d'algorithmes très sophistiqués dont la compréhension est inaccessible à la majorité des utilisateurs. Il faut sans doute aussi retenir un déficit de formation des utilisateurs.

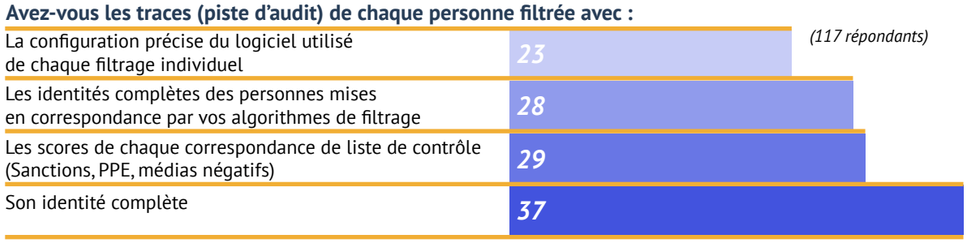
3 - Les utilisateurs sont plutôt appliqués dans la qualification des alertes

A. Pour 56% des sondés, une alerte est traitée dans un délai inférieur à une journée
B. 70% des sondés passent plus de 10 minutes à traiter une alerte (voir nos remarques sur le point 2)
C. 40 % des alertes sont documentées avec des explications sur le nom, le prénom et la date de naissance et 30% avec des pièces jointes comme des pièces d'identité
D. 30% des alertes sont documentées avec l'aide d'un superviseur ou d'un expert.

4 - La piste d'audit est une fonction clé mais perfectible

A. 86% des sondés considèrent la piste d'audit comme une fonction critique
B. De nombreux manquements demeurent dans les solutions utilisées par les sondés

Avez-vous les traces (piste d'audit) de chaque personne filtrée avec :

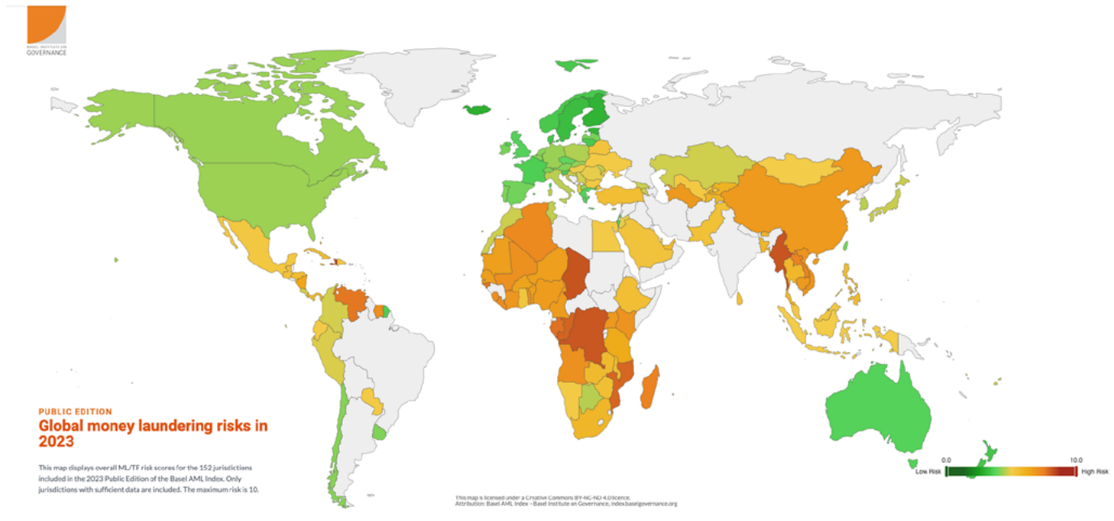


(117 répondants)

CHAPITRE 2

CRIMINALITÉ FINANCIÈRE, CONTEXTE ET HISTOIRE

La criminalité financière est mondiale complexe, elle englobe une vaste gamme d'activités illégales. Elle inclut, sans s'y limiter, le blanchiment d'argent, le financement du terrorisme, la fraude financière, la corruption, et l'évasion fiscale.
Cette carte affiche les scores globaux de risque de BC/FT pour les 152 juridictions incluses dans l'édition publique 2023 de l'indice Bâle AML[2].



[2] https://baselgovernance.org/basel-aml-index

Le blanchiment d'argent est le processus par lequel les criminels dissimulent l'origine illégale de leurs revenus, en les faisant transiter à travers des structures financières complexes pour leur donner une apparence légitime. On estime que le montant de l'argent blanchi chaque année représente 1 à 3% du PIB mondial[3] .

Les méthodes de blanchiment d'argent s'articulent autour de 3 étapes et de diverses techniques :

Les 3 étapes du blanchiment d'argent

ETAPE N°1 « Placement » : L'étape de placement est cruciale dans le processus de blanchiment d'argent. C'est la phase où l'argent illégalement acquis est introduit dans le système financier. Le but est de dissiper la trace directe entre les criminels et leur argent en la rendant moins suspecte ou invisible.

ETAPE N°2 « Empilement (ou Stratification) » : L'étape d'empilement, ou stratification, est la deuxième phase du processus de blanchiment d'argent : les fonds déjà introduits dans le système financier (lors de l'étape de placement) subissent une série de transactions complexes pour dissimuler leur origine illicite. Cette étape vise à brouiller les pistes, et à compliquer la traçabilité de l'argent. L'objectif de l'étape d'empilement est de séparer l'argent de sa source illégale par une confusion et une complexité telles que même si l'argent est identifié, il est difficile de relier ces fonds à des activités criminelles spécifiques. Cette étape requiert souvent une expertise financière et l'utilisation de techniques sophistiquées pour réussir à brouiller les pistes efficacement.

ETAPE N°3 : « Intégration » : L'étape d'intégration est la dernière phase du processus de blanchiment d'argent : les fonds blanchis sont réintroduits dans l'économie sous une apparence légitime. À ce stade, l'argent a été suffisamment dissimulé pour compliquer la détection de son origine illégale, et il peut être utilisé sans éveiller de soupçons.

[3] À l'échelle de l'Europe, Europol estime que les transactions suspectes représentent un montant de plusieurs centaines de milliards d'euros, qui équivaudrait à 1,3 % du produit intérieur brut (PIB) de l'UE. Au niveau mondial, les estimations font état d'un taux proche de 3 % du PIB de la planète. Source : L'UE et la lutte contre le blanchiment de capitaux dans le secteur bancaire : des efforts fragmentés et une mise en œuvre insuffisante.

Les techniques de blanchiment d'argent

Les techniques utilisées au cours de ces étapes sont multiples et recourent à des opérations empruntées à différents secteurs d'activités.
Dans le cadre de l'application des exigences réglementaires dans les domaines du Gel des avoirs, et des PPE, Il est utile de connaître ces opérations car l'obligation de détection de personnes sous sanction ou politiquement exposées s'applique à la fois au portefeuille de relations d'affaires et aux opérations de ces dites relations d'affaires.
Les rapports annuels du Tracfin où sont présentés des cas typologiques de blanchiment sont riches en information sur les différentes techniques utilisées.

ASSURANCE	Souscription et rachat rapide (anticipé) de polices d'assurance-vie Utilisation de contrats d'assurance pour transférer des fonds dans des pays tiers Polices d'assurance avec bénéficiaires suspects ou changements fréquents de bénéficiaires Transactions inhabituelles impliquant des sociétés d'assurance offshore Surprime ou sur-paiement de polices d'assurance avec demande de remboursement Contrats d'assurance associés à des prêts ou à des garanties bancaires Blanchiment via commissions Création de sinistres fictifs
BANQUE	Dépôts fractionnés (Smurfing) Transferts internationaux suspects et chaînes de transferts Comptes dormants soudainement actifs Utilisation de sociétés écrans Transactions incohérentes avec le profil du client Prêts fictifs ou dos-à-dos Flux financiers fragmentés Usage anormal de produits bancaires (chèques de banque, lettres de crédit, ...) Opérations impliquant des intermédiaires financiers
FINANCE	Transactions impliquant des instruments financiers complexes Utilisation de sociétés offshore et de structures d'entreprise complexe Opérations de marché suspectes ; « pump and dump » (gonfler et vendre), ou le trading d'initiés. Placement et gestion de fonds en provenance de sources inconnues ou suspectes Investissements dans des biens de haute valeur Utilisation de produits d'investissement alternatifs Transactions inter-entreprises inexpliquées Participations dans des entreprises via des intermédiaires Utilisation de fonds de placements privés
IMMOBILIER	Transactions immobilières à valeur incohérente Achats répétés et rapides de propriétés (flipping) Utilisation de sociétés écrans ou de prête-noms Paiements anormaux ou en espèces Financements et prêts suspects Investissements immobiliers internationaux Location de propriétés avec revenus fictif
JEUX	Achat de jetons de casino avec des fonds illicites Utilisation de machines à sous ou de jeux de table Transferts de fonds entre les comptes de joueurs en ligne Participation à des tournois de poker Gains de jeux gonflés ou fictifs Utilisation de prête-noms ou de comptes multiples Achats inexpliqués de tickets de loterie Jeux en ligne et paiements électroniques
COMMERCE	Surfacturation ou sous-facturation Commerce basé sur des documents fictifs Entreprises de façade Commerce international et import-export Utilisation de comptes bancaires d'entreprises pour des transactions personnelles Transactions en espèces importantes Transferts rapides de propriété d'entreprise Commerce de biens de haute valeur

Les Personnes Politiquement Exposées (1990)

La notion de « personne politiquement exposée » (PPE) est apparue dans les années 90 en réponse à la nécessité de renforcer la lutte contre le blanchiment d'argent et le financement du terrorisme.

Elle tient compte des risques particuliers liés aux personnes occupant des postes politiques élevés et à leurs possibilités de détourner des fonds publics ou encore de recevoir des fonds illicites en contrepartie de « services » qui relèvent de la corruption.

L'origine de cette notion peut être retracée à travers les initiatives internationales visant à améliorer la transparence financière, et à prévenir la corruption, et peut être attribuée à plusieurs développements clés :

1. INITIATIVE DE LUTTE CONTRE LA CORRUPTION :
Dans les années 1990, il y a eu une prise de conscience croissante au niveau international de l'importance de la lutte contre la corruption, en particulier dans le secteur public. Des organisations internationales telles que les Nations Unies et l'Organisation de coopération et de développement économiques (OCDE) ont commencé à travailler sur des initiatives de lutte contre la corruption.

2. NORMES INTERNATIONALES DE LUTTE CONTRE LE BLANCHIMENT D'ARGENT :
Parallèlement à la lutte contre la corruption, il y a eu un effort pour établir des normes internationales de lutte contre le blanchiment d'argent. Le Groupe d'action financière (GAFI), une organisation intergouvernementale, a joué un rôle clé dans l'élaboration de ces normes. Le GAFI a commencé à élaborer des recommandations pour la lutte contre le blanchiment d'argent dans les années 1990.

3. RECONNAISSANCE DES RISQUES LIÉS AUX PPE :
Au fur et à mesure que les travaux sur les normes de lutte contre le blanchiment d'argent avançaient, il est devenu évident que les personnes occupant des postes[4] politiques élevés, y compris les chefs d'État, les ministres, les hauts fonctionnaires et leurs proches, pouvaient être particulièrement vulnérables à la corruption et au blanchiment d'argent. Ils avaient également la capacité de dissimuler des fonds illicites.

4. INTÉGRATION DE LA NOTION DE PPE :
Pour répondre à ces risques spécifiques, le GAFI et d'autres organismes ont intégré la notion de «personne politiquement exposée» dans leurs recommandations. Cette notion a été définie de manière à englober les individus occupant des fonctions gouvernementales ou politiques importantes et leurs proches. Il est important de noter que la définition des PPE peut varier assez sensiblement d'un pays à l'autre[5] en fonction de la façon dont chaque juridiction nationale met en œuvre les recommandations du GAFI. Cependant, le concept fondamental de la PPE en tant que personne occupant ou ayant occupé une fonction politique importante est resté constant depuis son introduction par le GAFI.

[4] Voir en annexe les fonctions visées par la réglementation française
[5] Ce qui peut représenter une difficulté dans l'application de la réglementation

Le Gel des Avoirs (1914)

La réglementation sur le gel des avoirs est une mesure utilisée par les gouvernements et les organisations internationales pour contraindre des entités (pays, entreprises, individus) à respecter certaines normes internationales ou à répondre de leurs actions. Cette pratique s'est développée et a évolué au fil des ans en réponse à divers conflits internationaux, actes de terrorisme, violations des droits humains, et activités criminelles telles que le blanchiment d'argent.

Voici un aperçu de l'histoire et du développement de la réglementation sur le gel des avoirs.

1. ORIGINE ET DÉVELOPPEMENT
Le concept de gel des avoirs remonte à la période des deux guerres mondiales, durant laquelle des pays ont utilisé cette tactique pour bloquer les avoirs des pays ennemis. Pendant la Première et la Seconde Guerre mondiale, de nombreux pays ont gelé les avoirs des nations adverses pour empêcher l'utilisation de ces ressources dans l'effort de guerre ennemi.

2. PENDANT LA GUERRE FROIDE
Avec la Guerre Froide, le gel des avoirs est devenu un outil de politique étrangère plus fréquemment utilisé, notamment dans le cadre des sanctions économiques. Les États-Unis et leurs alliés ont par exemple utilisé le gel des avoirs comme moyen de pression sur l'Union Soviétique et d'autres pays alignés.

3.LUTTE CONTRE LE TERRORISME ET LE BLANCHIMENT D'ARGENT
À la fin du 20e et au début du 21e siècle, le gel des avoirs est devenu un outil clé dans la lutte contre le terrorisme et le blanchiment d'argent. Après les attentats du 11 septembre 2001, de nombreux pays et organisations internationales, comme les Nations Unies et l'Union européenne, ont adopté des réglementations strictes pour geler les avoirs des individus et des organisations suspectés de terrorisme.

4. SANCTIONS INTERNATIONALES
Le gel des avoirs est également un élément important des sanctions internationales contre les pays qui violent le droit international, les droits de l'homme, ou qui menacent la paix et la sécurité internationales. Des exemples récents incluent les sanctions contre l'Iran, la Corée du Nord, et la Russie, où les avoirs d'entités et individus ont été gelés dans le cadre de mesures punitives plus larges.

5.CADRE LÉGAL ET COOPÉRATION INTERNATIONALE
La réglementation sur le gel des avoirs repose sur divers cadres légaux internationaux, régionaux et nationaux. Les résolutions du Conseil de sécurité des Nations Unies, les directives de l'Union européenne, et les lois nationales fournissent le cadre juridique pour la mise en œuvre des mesures de gel des avoirs. La coopération internationale, notamment à travers le Groupe d'action financière (GAFI), est cruciale pour l'efficacité de ces mesures.

Cette réglementation sur le gel des avoirs continue d'évoluer, s'adaptant aux défis mondiaux émergents et aux nouvelles menaces pour la paix et la sécurité internationales. Elle reste un outil diplomatique et économique essentiel pour les gouvernements et les organisations internationales dans leurs efforts pour maintenir ou restaurer l'ordre international.

La Réglementation dans les domaines du gel des avoirs et des PPE

La réglementation en matière de lutte contre la criminalité financière est un élément essentiel de ce paysage. Des organismes internationaux tels que le Groupe d'action financière (GAFI) établissent des normes mondiales, tandis que les réglementations locales varient d'un pays à l'autre.

En France, la réglementation fait l'objet d'une déclinaison des règles selon 5 niveaux :

Le niveau International
Le niveau européen
Le niveau national
Le niveau des autorités administratives
Le niveau des autorités de contrôle

1. LE NIVEAU INTERNATIONAL :

Pour ce niveau, nous retiendrons les dispositions de l'ONU et du GAFI.

A) L' ONU

Les sanctions du Conseil de sécurité prennent diverses formes et visent divers objectifs. Elles vont des sanctions économiques et commerciales de vaste portée à des mesures plus ciblées, telles que des embargos sur les armes, des interdictions de voyager et des restrictions financières ou frappant les produits de base.
Le Conseil de sécurité a appliqué des sanctions pour appuyer les transitions pacifiques, décourager les changements non constitutionnels, lutter contre le terrorisme, protéger les droits de l'homme et promouvoir la non-prolifération[6].

A.1) ONU ET GEL DES AVOIRS

Les sanctions internationales sont souvent imposées par le Conseil de sécurité des Nations Unies en réponse à des menaces pour la paix et la sécurité internationales. La liste de tous les régimes de sanctions sur décision de l'ONU est disponible sur le site du Trésor[7], dans les FAQ du registre des sanctions.
Ces résolutions du Conseil de sécurité des Nations Unies imposent souvent des sanctions telles que le gel des avoirs, l'embargo sur les armes, l'interdiction de voyager, et d'autres mesures similaires pour tenter de résoudre des crises internationales et de maintenir la paix et la sécurité internationales. Il est important de noter que la liste des sanctions et des résolutions évolue au fil du temps en réponse à l'évolution de la situation internationale.

A.2) ONU ET PPE

Les principales initiatives de l'ONU concernant les PPE visent à prévenir la corruption et à promouvoir la transparence. Voici quelques-uns des principaux textes et initiatives de l'ONU dans ce domaine :

- **Convention des Nations Unies contre la corruption (CNUCC) :**
La CNUCC, adoptée en 2003, comprend des dispositions relatives aux PPE. Elle appelle les États membres à prendre des mesures pour prévenir la corruption parmi les personnes politiquement exposées et à établir des mécanismes pour surveiller leurs transactions financières.

- **Les Principes directeurs des Nations Unies pour la lutte contre la corruption :**
Ces principes, élaborés par l'ONU, fournissent des orientations aux États membres sur la manière de prévenir et de lutter contre la corruption. Ils incluent des dispositions spécifiques sur la prévention de la corruption parmi les PPE.

- **Principes de la Banque mondiale pour la gestion des risques de corruption liés aux projets de développement :**
La Banque mondiale a élaboré ces principes pour aider à identifier et à gérer les risques de corruption dans le cadre de projets de développement. Ils incluent des dispositions pour la gestion des risques liés aux PPE dans le contexte de l'aide au développement.

- **Programme des Nations Unies pour le développement (PNUD) :**
Le PNUD travaille sur des initiatives visant à renforcer la gouvernance, à prévenir la corruption et à promouvoir la transparence dans les pays du monde entier. Cela peut inclure des programmes visant à aider les pays à mettre en œuvre des mesures pour lutter contre la corruption parmi les PPE.

Ces textes et initiatives de l'ONU visent à promouvoir la transparence, à prévenir la corruption et à renforcer la gouvernance, en particulier dans le contexte des personnes politiquement exposées, qui sont considérées comme présentant un risque accru de corruption en raison de leur accès aux ressources et au pouvoir gouvernemental.

[6] https://www.un.org/securitycouncil/fr/sanctions/information
[7] https://www.tresor.economie.gouv.fr/services-aux-entreprises/sanctions-economiques/registre-national-des-gels-foire-aux-questions

B) LE GAFI

Le dispositif de l'ONU est essentiellement complété au niveau international par celui du Groupe d'Action Financière dit GAFI[8].
Le Groupe d'action financière (GAFI) est une organisation mondiale de surveillance du blanchiment de capitaux et du financement du terrorisme. Cette organisation intergouvernementale fixe des normes internationales visant à prévenir ces activités illégales et les dommages qu'elles causent à la société. En tant qu'organe d'élaboration des politiques, le GAFI s'efforce de susciter la volonté politique nécessaire à la mise en œuvre de réformes législatives et réglementaires nationales dans ces domaines.
L'organisation, qui compte 40 membres, définit des normes internationales afin de garantir que les autorités nationales puissent s'attaquer efficacement aux fonds illicites liés au trafic de drogue, au commerce illicite des armes, à la cyberfraude et à d'autres crimes graves. Au total, plus de 200 pays et juridictions se sont engagés à mettre en œuvre les normes du GAFI dans le cadre d'une réponse mondiale coordonnée visant à prévenir le crime organisé, la corruption et le terrorisme.

B.1) GAFI ET GEL DES AVOIRS

Le GAFI a présenté 9 recommandations spéciales dans le domaine du Gel des avoirs. Reconnaissant l'importance vitale de prendre des mesures afin de lutter contre le financement du terrorisme, le GAFI a adopté ces 9 recommandations spéciales qui, conjointement à ses quarante recommandations sur le blanchiment de capitaux, fournissent le cadre fondamental visant à détecter, prévenir et réprimer le financement du terrorisme et des actes terroristes[9].

Voici ces 9 recommandations :

I. Ratification et mise en œuvre des instruments des Nations Unies
Chaque pays doit prendre les mesures immédiates pour ratifier et pour mettre en œuvre sans restriction la Convention de 1999 des Nations Unies pour la répression du financement du terrorisme. Les pays doivent également mettre en œuvre immédiatement les résolutions des Nations Unies relatives à la prévention et la répression du financement des actes terroristes, notamment la Résolution 1373 du Conseil de sécurité des Nations Unies.

II. Incrimination du financement du terrorisme et du blanchiment de capitaux commis dans le cadre des activités terroristes
Chaque pays doit ériger en infraction pénale le financement du terrorisme, des actes terroristes et des organisations terroristes
Les pays doivent s'assurer que de telles infractions sont désignées comme des infractions sous-jacentes au blanchiment de capitaux.

[8] https://www.fatf-gafi.org/fr/the-fatf/who-we-are.html
[9] https://www.fatf-gafi.org/fr/publications/Recommandationsgafi/Lesixrecommandationsspeciales.html

III. Gel et confiscation des biens terroristes

Chaque pays doit mettre en œuvre des mesures pour geler sans délai les fonds ou autres biens des terroristes et de ceux qui financent le terrorisme et les organisations terroristes, conformément aux résolutions des Nations Unies relatives à la prévention et la répression du financement des actes terroristes.

Chaque pays doit également adopter et mettre en œuvre des mesures, y compris de nature législative, afin de permettre aux autorités compétentes de saisir et de confisquer les biens qui sont utilisés pour, ou destinés ou alloués à être utilisés pour le financement du terrorisme, des actes terroristes ou des organisations terroristes, ou qui en constituent le produit.

IV. Déclaration des transactions suspectes liées au terrorisme

Si les institutions financières, ou les autres entreprises ou entités assujetties aux obligations relatives à la lutte contre le blanchiment de capitaux, suspectent, ou ont des motifs raisonnables de suspecter que des fonds sont liés, associés ou destinés à être utilisés pour le financement du terrorisme, des actes terroristes ou des organisations terroristes, elles doivent être tenues de déclarer rapidement leurs soupçons aux autorités compétentes.

V. Coopération Internationale

Chaque pays doit apporter aux autres pays, sur le fondement d'un traité, d'un accord ou de tout autre mécanisme relatif à l'entraide judiciaire ou à l'échange de renseignements, l'assistance la plus large possible dans le cadre des enquêtes, investigations ou procédures pénales, civiles ou administratives concernant le financement du terrorisme, des actes terroristes et des organisations terroristes.

Les pays doivent également prendre toutes les mesures possibles en vue d'assurer qu'ils ne fournissent pas de refuge aux personnes poursuivies pour le financement du terrorisme, des actes terroristes, ou des organisations terroristes, et ils devraient mettre en œuvre, dans la mesure du possible, des procédures permettant l'extradition de telles personnes.

VI. Remise de fonds alternative

Chaque pays doit prendre des mesures afin de s'assurer que les personnes physiques ou morales, y compris les agents, qui fournissent un service de transmission de fonds ou de valeurs, y compris la transmission à travers un système ou réseau informel visant le transfert de fonds ou de valeurs, obtiennent une autorisation d'exercer ou s'inscrivent sur un registre, et qu'elles soient assujetties à toutes les recommandations du GAFI qui s'appliquent aux banques et aux institutions financières non bancaires.

Chaque pays doit s'assurer que les personnes physiques ou morales qui fournissent ce service illégalement soient passibles de sanctions administratives, civiles ou pénales.

VII. Virements électroniques

Les pays doivent prendre des mesures afin d'obliger les institutions financières, y compris les services de remise de fonds, à inclure des renseignements exacts et utiles relatifs au donneur d'ordre (nom, adresse et numéro de compte) concernant les transferts de fonds et l'envoi des messages qui s'y rapportent. Les renseignements doivent accompagner le transfert ou le message qui s'y rapporte tout au long de la chaîne de paiement.

Les pays doivent prendre des mesures pour s'assurer que les institutions financières, y compris les services de remise de fonds, mettent en œuvre une surveillance approfondie et un suivi aux fins de détection des activités suspectes des transferts de fonds non accompagnés de renseignements complets sur le donneur d'ordre (nom, adresse et numéro de compte).

VIII. Organismes á but non lucratif

Les pays doivent entreprendre une revue de l'adéquation de leurs lois et réglementations relatives aux entités qui peuvent être utilisées afin de financer le terrorisme.

IX. Les passeurs du fonds « Cash Couriers »

Les pays doivent avoir en place des mesures destinées à détecter les transports physiques transfrontaliers d'espèces et instruments au porteur, y compris un système de déclaration ou toute autre obligation de communication.

Les pays doivent s'assurer que leurs autorités compétentes sont dotées du pouvoir de bloquer ou retenir les espèces ou instruments au porteur soupçonnés d'être liés au financement du terrorisme ou au blanchiment de capitaux, ou faisant l'objet de fausses déclarations ou communications.

Les pays doivent s'assurer que des sanctions efficaces, proportionnées et dissuasives peuvent s'appliquer aux personnes qui ont procédé à des fausses déclarations ou communications. Lorsque des espèces ou instruments au porteur sont liés au financement du terrorisme ou au blanchiment de capitaux, les pays devraient aussi adopter des mesures, y compris de nature législative, conformes à la Recommandation 3 et à la Recommandation spéciale III, qui autorisent la confiscation de telles espèces ou de tels instruments.

B.2) GAFI ET PPE

La Recommandation 12 (R12) Personnes politiquement exposées (PPE) traite spécifiquement des personnes politiquement exposées avec les points clés suivants :

- **Identification des PPE :**

Les institutions financières et les professionnels de la lutte contre le blanchiment d'argent (PLBA) doivent mettre en place des procédures pour identifier leurs clients qui sont des PPE, ainsi que les membres de leur famille proche.

- **Évaluation du Risque :**

Les institutions financières et les PLBA doivent effectuer une évaluation appropriée du risque associé aux PPE, en tenant compte de leur position, de leur fonction et de leur relation avec le client.

- **Diligence Raisonnable Renforcée (DDR) :**

Lorsqu'il est identifié qu'un client est une PPE, les institutions financières et les PLBA doivent appliquer une diligence raisonnable renforcée (DDR) pour comprendre la source de la richesse et des fonds de cette personne, ainsi que la finalité de la relation d'affaires.

- **Obligations de Déclaration :**

Les institutions financières et les PLBA doivent avoir des obligations de déclaration aux autorités compétentes en cas de transactions suspectes ou inhabituelles impliquant des PPE.

- **Mesures Complémentaires :**

Les pays membres du GAFI sont encouragés à prendre des mesures complémentaires, telles que l'adoption de lois et de réglementations spécifiques sur les PPE et la publication de directives pour les institutions financières.

La Réglementation dans les domaines du gel des avoirs et des PPE

2. LE NIVEAU EUROPÉEN :

Le deuxième niveau est celui de l'Europe dont le cadre réglementaire se compose de règlements, de directives et de plans d'action.

En 20 ans, 6 directives européennes ont été mises en place[10]. En résumé :

Directive n°1 (juin 1991) :

1AMLD était une première étape dans la réglementation de l'UE en matière de LAB et de LFT, établissant des normes minimales pour les institutions financières et les professionnels.

Elle introduisait des obligations de diligence raisonnable, de déclaration des transactions suspectes, d'identification des clients, et elle prévoyait la possibilité d'imposer des sanctions en cas de non-conformité.

Cette directive a posé les bases de la législation ultérieure de l'UE visant à renforcer la lutte contre le blanchiment d'argent et le financement du terrorisme.

[10] https://www.mazars.fr/insights/publications-et-evenements/avis-d-experts/lutte-anti-blanchiment-focus-sur-la-5e-directive

LE POINT DE VUE D'ASTRÉE AVOCATS

L'IMPRÉCISION DES TEXTES ET L'INEXACTITUDE DES DONNÉES EST PROBLÉMATIQUE

La réglementation relative au gel des avoirs et aux personnes politiquement exposées soulève aujourd'hui de nombreuses interrogations pratiques et éthiques.

Tout d'abord, s'agissant de l'application pratique de ces règles, beaucoup d'entités soumises à la LCB-FT ont aujourd'hui des difficultés à respecter leur obligation de connaissance clientèle et à disposer de données exactes. Or, il est primordial dans l'application de la réglementation PPE/GDA de disposer de telles données pour avoir un filtrage efficace.

En outre, des difficultés naissent également en raison de l'imprécision des textes : la définition des personnes politiquement exposées de niveau 2 ou 3 est ainsi trop large et impossible à mettre en pratique (voir article R.561-18 du CMF conjoint, concubin du PPE, relation d'affaires..)

S'agissant des interrogations éthiques, il apparaît que la mise en œuvre d'une telle réglementation intervient parfois en contradiction avec d'autres règles de droit.
Par exemple, le risque de données inexactes étant très important un manquement au RGPD peut être caractérisé, ce que le Comité Européen de la protection européenne n'a pas manqué de rappeler dans une lettre du 20 mai 2022.

Enfin, des données inexactes peuvent également donner lieu à des manquements graves à la présomption d'innocence comme ce fut le cas en 2017 avec un prestataire qui utilisait des listes comprenant des fausses données.

https://www.lalibre.be/belgique/2017/06/24/16000-belges-se-trouveraient-sur-la-liste-noire-des-banques-4UJLYLN4ABH4VHWZ4463EYF7TQ/

Directive n°2 (décembre 2001) :
La deuxième directive anti-blanchiment de l'UE (2AMLD) a élargi la portée des règles de LAB et de LFT, renforcé le rôle des autorités de surveillance, introduit des exigences concernant l'identification des propriétaires réels, permis l'identification à distance des clients, renforcé les sanctions et encouragé la coopération entre les États membres.

Directive n°3 (octobre 2005) :
La 3AMLD a renforcé la réglementation de l'UE en matière de LAB et de LFT par rapport aux directives précédentes en introduisant des exigences spécifiques pour les PPE, des registres des bénéficiaires effectifs, des évaluations des risques, des sanctions accrues, et en encourageant la coopération et l'échange d'informations entre les États membres.

Directive n°4 (juin 2015) :
La 4AMLD a renforcé considérablement la législation de l'UE en matière de LAB et de LFT en introduisant des sanctions pénales plus sévères, en élargissant la responsabilité des personnes morales, en facilitant la confiscation des produits du crime, en élargissant la portée des infractions et en encourageant la coopération entre les États membres de l'UE pour lutter plus efficacement contre ces activités illicites. Elle renforce également la transparence en ce qui concerne la propriété réelle des entreprises et des trusts.

Directive n°5 (mai 2018) :
La 5AMLD élargit la définition des PPE, renforce les obligations relatives aux registres des bénéficiaires effectifs, encourage la coopération entre les États membres, renforce la lutte contre le financement du terrorisme, élargit sa portée aux crypto-actifs et impose des sanctions plus sévères.

Directive n°6 (octobre 2018) :
La 6ème directive européenne contre le blanchiment d'argent, également connue sous le nom de 6AMLD, apporte plusieurs changements significatifs dans la lutte contre le blanchiment d'argent et le financement du terrorisme au sein de l'Union européenne.

Voici les principaux apports de cette dernière directive :

- **Harmonisation des Définitions de Blanchiment d'Argent :**
La 6AMLD harmonise la définition du blanchiment d'argent dans toute l'UE, éliminant les lacunes dans la législation nationale des États membres. Elle inclut une liste harmonisée de 22 infractions principales qui constituent le blanchiment d'argent, y compris certains délits fiscaux, la criminalité environnementale et la cybercriminalité.

- **Élargissement du Champ d'Application Réglementaire :**
La directive élargit le nombre d'infractions qui entrent dans la définition du blanchiment d'argent. La complicité, l'incitation au blanchiment d'argent, et les tentatives de blanchiment sont désormais incluses et sujettes à des sanctions pénales.

- **Extension de la Responsabilité Pénale :**
La 6AMLD étend la responsabilité pénale aux personnes morales, telles que les sociétés ou les partenariats. Si un « esprit dirigeant » de l'entreprise mène une activité illégale de blanchiment d'argent, l'entreprise peut être tenue responsable.

- **Sanctions Plus Sévères :**
La directive introduit une peine de prison minimale de quatre ans pour les infractions de blanchiment d'argent, une augmentation par rapport à la peine minimale précédente d'un an. Elle donne également aux juges le pouvoir d'infliger des amendes aux personnes physiques et d'exclure les entités de l'accès aux financements publics.

- **Mesures Spécifiques :**
Des mesures telles que la limitation des paiements en espèces à 10 000 euros, des règles de transparence pour les clubs de football, et des pouvoirs accrus pour les cellules de renseignement financier sont également incluses. Ces cellules auront la responsabilité de prévenir, signaler et lutter contre le blanchiment d'argent et le financement du terrorisme.

- **Accessibilité des Informations :**
Les informations sur les bénéficiaires effectifs seront plus accessibles, ce qui aidera à détecter rapidement les dispositifs de blanchiment de capitaux et à geler les avoirs.

LE LIVRE BLANC
LA RÉGLEMENTATION GDA & PPE
NIVEAU EUROPÉEN

LE POINT DE VUE D'ASTRÉE AVOCATS

LCB-FT ET RESPONSABLITÉ PÉNALE

La 6ème directive a étendu les définitions de blanchiment d'argent et de responsabilité pénale.
Pour le dispositif LCB-FT aucun changement significatif n'est à noter.
En revanche, cette directive étend la responsabilité pénale aux personnes morales et aux membres de la direction des entités soumises à la LCB-FT, notamment dans les cas de blanchiment où aucune mesure n'a été prise. Cette extension caractérise une volonté accrue de sanctionner ceux qui ne respectent pas leurs obligations LCB-FT.
Point important : le législateur français n'a pas eu à transposer en droit interne les évolutions qu'elle contient, les dispositions du droit pénal national étant jugées d'ores et déjà suffisamment conformes aux exigences de la directive.
Un nouveau paquet législatif LCB-FT sera prochainement adopté par les autorités européennes avec de nombreux ajouts relatifs à la LCB-FT, aux bénéficiaires effectifs et à une nouvelle autorité européenne, l'ALBC, qui sera située à Francfort.

https://www.consilium.europa.eu/en/press/press-releases/2024/01/18/anti-money-laundering-council-and-parliament-strike-deal-on-stricter-rules

La Réglementation dans les domaines du Gel Des Avoirs et des Personnes Politiquement Exposées

L'UE ET LE GEL DES AVOIRS

Les décisions de l'UE dans le domaine du gel des avoirs sont la fois communes et complémentaires de celles de l'ONU. Le processus d'adoption des mesures restrictives par le Conseil de l'Union européenne dans le cadre de la Politique Étrangère et de Sécurité Commune (PESC) suit les étapes suivantes :

1. **Proposition de mesures restrictives :** Le haut représentant de l'Union pour les affaires étrangères et la politique de sécurité (HR) propose des mesures restrictives. Ces propositions sont examinées par des groupes compétents selon la région géographique concernée, le groupe RELEX (conseillers pour les relations extérieures), le Comité politique et de sécurité (COPS) si nécessaire, et le Comité des représentants permanents (Coreper II).

2. **Adoption par le Conseil** : La décision est adoptée à l'unanimité par le Conseil. Si elle inclut un gel des avoirs ou d'autres sanctions économiques/financières, elle doit être mise en œuvre par un règlement du Conseil.

3. **Adoption d'un règlement du Conseil** : Sur la base de la décision PESC, le haut représentant de l'Union pour les affaires étrangères et la politique de sécurité (HR) et la Commission soumettent une proposition de règlement qui est examinée par le groupe des conseillers pour les relations extérieures (RELEX), puis transmise au Comité des représentants permanents (Coreper) et au Conseil pour adoption. Le Conseil informe le Parlement européen de cette adoption.

4. **Champ d'application et mise en œuvre** : Le règlement définit le champ d'application des mesures et les modalités de leur mise en œuvre. Il est contraignant pour toutes les personnes et entités au sein de l'UE.

5. **Entrée en vigueur :** La décision du Conseil est effective dès sa publication au Journal officiel de l'Union européenne. Les mesures de la décision PESC et le règlement du Conseil sont adoptés simultanément.

6. **Mise en œuvre des mesures** : Les embargos sur les armes ou les restrictions de déplacement, par exemple, sont mises en œuvre par les États membres, avec la Commission vérifiant leur application adéquate.

7. **Procédure de notification et de réexamen** : Les personnes et entités affectées sont informées par courrier ou via une publication officielle. Les mesures restrictives font l'objet d'un réexamen constant.

8. **Résolutions du Conseil de Sécurité des Nations Unies et régimes sSanctions mixtes** : Les mesures liées aux résolutions de l'ONU n'ont pas de date limite et sont réexaminées ou modifiées selon les décisions de l'ONU. Les sanctions mixtes de l'ONU et de l'UE sont également soumises à réexamen. Une décision de l'ONU ne se retrouve pas immédiatement dans une liste dite consolidée UE ou FR. Il faut donc prendre soin d'utiliser ces différentes listes qui par ailleurs ne sont pas renseignées de la même façon

9. **Mesures restrictives autonomes** : Ces mesures durent généralement 12 mois et sont réexaminées avant toute prolongation, modification, ou suspension.

10. **Demande de levée de mesures restrictives** : Les personnes et entités listées peuvent demander un réexamen de leur situation au Conseil, en fournissant les justificatifs nécessaires.

La liste de tous les régimes de sanction sur décision de l'UE est disponible sur le site du Trésor[12], dans les FAQ du registre des sanctions.

[12] https://www.tresor.economie.gouv.fr/services-aux-entreprises/sanctions-economiques/registre-national-des-gels-foire-aux-questions

LE LIVRE BLANC
LA RÉGLEMENTATION GDA & PPE
NIVEAU EUROPÉEN

LE POINT DE VUE D'ASTRÉE AVOCATS

> **L'IMPORTANCE DES LISTES AUTONOMES POUR TENIR COMPTE DES DÉLAIS DE PARUTION.**

En raison d'une actualité particulièrement sous tension (guerre en Ukraine, attentats…) les listes de gel des avoirs évoluent en permanence et sont régulièrement mises à jour.

A tout moment, l'Organisation des Nations Unies, l'Union Européenne ou le Gouvernement Français peuvent prendre des nouvelles mesures restrictives.

Il est donc crucial de disposer de listes autonomes afin de tenir compte des délais de parution spécifiques à chaque liste.

La Réglementation dans les domaines du gel des avoirs et des PPE

L'UE ET LES PPE

Les principales dispositions législatives et réglementaires de l'UE relatives aux PPE sont les suivantes :

1. **Quatrième directive anti-blanchiment (4AMLD)** : Elle a établi des règles spécifiques pour l'identification et la diligence raisonnable à l'égard des PPE, ainsi que pour leurs proches.

2. **Cinquième directive anti-blanchiment (5AMLD)** : Elle a élargi la définition des PPE pour inclure les personnes exerçant des fonctions politiques nationales et étrangères, et a introduit des règles plus strictes en matière de diligence raisonnable, de communication et de conservation des informations. Les États membres sont tenus de créer et de publier les listes PPE officielles qui comprennent les titres, les rôles et les fonctions considérés comme politiquement exposés.

3. **Règlement (UE) n° 2015/847** : Ce règlement, adopté en 2015, concerne les transferts électroniques de fonds et établit des normes pour l'identification et la vérification de l'identité des PPE et de leurs proches dans le cadre de ces transferts.

LE POINT DE VUE D'ASTRÉE AVOCATS

> **L'UE TRAVAILLE À LA PUBLICATION DE VÉRITABLES LISTES DE PPE**

Contrairement aux listes de Gel des avoirs, il n'existe pas de listes nominatives des personnes politiquement exposées (PPE).
L'état fournit uniquement les fonctions ou titres considérés comme PPE.

En conséquence, il est primordial de disposer de listes de filtrage qui soient le plus exactes possible pour avoir un filtrage efficace et pour éviter tout manquement aux droits des personnes (vie privée, présomption d'innocence, etc).

L'Union Européenne travaille actuellement à la publication de listes de PPE consolidées afin de résoudre ce problème. Aucune date précise n'a en revanche été avancée.

La Réglementation dans les domaines du gel des avoirs et des PPE

3. LE NIVEAU NATIONAL :

3A) LE GEL DES AVOIRS EN FRANCE
En quelques lignes voici, les principales mesures qui ont marqué le dispositif gel des avoirs en France.

Années 1990
Mesures initiales : La France a commencé à adopter des mesures de gel des avoirs en réponse aux résolutions du Conseil de sécurité des Nations unies, notamment concernant des sanctions contre certains pays ou entités. Ces mesures étaient principalement axées sur des sanctions internationales.

Après le 11 septembre 2001
La lutte contre le financement du terrorisme est devenue une priorité majeure. La France, comme d'autres pays, a renforcé ses dispositifs législatifs et réglementaires pour geler les avoirs des individus et des organisations liés au terrorisme, en réponse aux résolutions de l'ONU et à des initiatives au niveau de l'Union européenne.

Loi du 9 juillet 2004
Cette loi, relative au gel des avoirs des personnes physiques ou morales impliquées dans des activités terroristes, a marqué un tournant, permettant au gouvernement français de geler les avoirs de ces entités sur son territoire.

Loi du 26 juillet 2005
Elle a introduit des mesures pour renforcer la lutte contre le financement du terrorisme, en particulier en facilitant le gel des avoirs.

Directive UE 2015/849
Bien que cette directive concerne principalement la lutte contre le blanchiment de capitaux et le financement du terrorisme, elle comprend des dispositions relatives au gel des avoirs.

Lois et règlements successifs
Au fil des années, la France a continué d'adapter sa législation pour se conformer aux standards internationaux et européens, et pour répondre aux évolutions des menaces de sécurité. Cela a inclus des ajustements réguliers des listes d'individus et d'entités dont les avoirs sont gelés.

Règlement Général sur la Protection des Données (RGPD)
Bien que non spécifiquement axé sur le gel des avoirs, le RGPD a eu un impact sur la manière dont les données personnelles sont traitées dans le cadre de ces mesures.

3B) LES PPE EN FRANCE
La réglementation française concernant les PPE s'est développée en parallèle des directives européennes et des recommandations internationales, en particulier celles du GAFI. Ceci reflète l'engagement croissant envers la transparence financière et la lutte contre le blanchiment de capitaux et le financement du terrorisme.

Il faut noter en particulier :

Ordonnance n° 2009-104 du 30 janvier 2009 :
Cette ordonnance a transposé en droit français la Troisième directive anti-blanchiment de l'UE, en intégrant des dispositions relatives aux PPE.

Ordonnance n° 2016-1635 du 1er décembre 2016 :
Elle a transposé la Quatrième directive anti-blanchiment dans le droit français, avec des dispositions spécifiques pour les PPE, notamment en ce qui concerne l'identification, l'évaluation des risques et les mesures de vigilance renforcées.

Loi n° 2018-898 du 23 octobre 2018 :
Cette loi, relative à la lutte contre la fraude, a inclus des mesures renforçant le contrôle des PPE, notamment en matière de déclaration de soupçon.

La Réglementation dans les domaines du gel des avoirs et des PPE

4. LE NIVEAU DES AUTORITÉS ADMINISTRATIVES :

Le quatrième niveau est le niveau des autorités administratives

En France, plusieurs organismes et autorités ont la responsabilité de lutter contre le blanchiment de capitaux.

Ces entités jouent différents rôles, allant de la réglementation et la supervision à l'enquête et la poursuite. Les principaux organismes impliqués sont :

TRACFIN
(Traitement du Renseignement et Action contre les Circuits Financiers clandestins)
Il s'agit d'un service de renseignement français rattaché au ministère de l'Économie et des Finances. TRACFIN est chargé de lutter contre le blanchiment d'argent, le financement du terrorisme, et les fraudes économiques et financières graves. Il analyse les informations suspectes et peut transmettre des dossiers aux autorités judiciaires.

L'ACPR
(Autorité de Contrôle Prudentiel et de Résolution)
Elle supervise les banques et les assurances et veille à ce que ces institutions respectent les règles de lutte LCB-FT.

L'AMF
(Autorité des Marchés Financiers)
L'AMF régule les participants et les produits des marchés financiers en France. Elle s'assure également du respect des obligations en matière de LCB-FT par les acteurs des marchés financiers.

LA CNS
(La commission nationale des sanctions)
La CNS est une institution indépendante chargée de sanctionner les manquements commis par certains professionnels (les agents immobiliers, les personnes exerçant l'activité de domiciliation et les opérateurs de jeux ou de paris, y compris en ligne), en ne respectant pas leurs obligations en matière de lutte contre le blanchiment des capitaux et le financement du terrorisme.

LA DGT
(Direction générale du Trésor)
Elle contribue à la définition des stratégies nationales dans ces domaines. La DGT représente aussi la France dans divers forums internationaux et groupes de travail liés aux finances, comme le Groupe d'Action Financière (GAFI). Elle joue un rôle dans la négociation et la mise en œuvre des standards internationaux en matière de LCB-FT. La Direction du Trésor contribue à l'élaboration des cadres réglementaires qui régissent les marchés, y compris les aspects liés à la lutte contre le blanchiment.

LES DOUANES FRANÇAISES
Elles jouent un rôle clé dans la détection et la prévention du blanchiment de capitaux, en particulier en contrôlant les

mouvements transfrontaliers d'espèces et de valeurs.

ORDRE DES AVOCATS, NOTAIRES ET AUTRES PROFESSIONS RÉGLEMENTÉES
Ces professions sont soumises à des obligations en matière de LCB-FT, notamment l'obligation de déclarer les soupçons de blanchiment à TRACFIN.

LE PNF
(Parquet National Financier)
Cette institution judiciaire est spécialisée dans la lutte contre la grande délinquance économique et financière, y compris le blanchiment de capitaux.

LA CRF
(Cellule de Renseignement Financier)
Bien que moins connue, cette cellule au sein de la Banque de France joue également un rôle dans la lutte contre le blanchiment de capitaux, en particulier en ce qui concerne les déclarations de soupçon émanant des institutions financières.

Police et Gendarmerie Nationales
Les services spécialisés de ces forces de l'ordre, tels que l'OCLCIFF (Office Central de Lutte contre la Corruption et les Infractions Financières et Fiscales), mènent des enquêtes sur les affaires de blanchiment de capitaux.

Notons que ces autorités sont à l'origine de textes de référence sans lesquels l'application des lois et des réglementations serait encore plus difficile.

Sur le gel de avoirs :
DGT : Guide de bonnes conduites / Foire aux questions relatifs à la mise en œuvre des sanctions économiques et financières[13]
DGT et ACPR : Lignes directrices[14]
Tracfin et DGCRF : Lignes directrices secteur de l'immobilier[15]
AMF : Guide[16]
Autres Secteurs : lignes directrices[17]

Sur les PPE
APCR : lignes directrices[18]
AMF : ligne directrices[19]

[13] https://www.tresor.economie.gouv.fr/Institutionnel/Niveau2/Pages/f3234489-26a1-48f7-8a05-f31d34551f13/files/d30c8579-086d-42e1-a43f-8b79a677dc46

[14] https://acpr.banque-france.fr/en-savoir-plus-sur-les-textes-utiles-en-lcb-ft

[15] https://www.economie.gouv.fr/files/LDimmobilier_VF_nov2018.pdf

[16] https://www.amf-france.org/fr/actualites-publications/publications/guides/guides-professionnels/guide-sur-le-gel-des-avoirs

[17] https://www.economie.gouv.fr/tracfin/lignes-directrices

[18] https://acpr.banque-france.fr/sites/default/files/media/2018/05/02/20180410_ld_ppe_college.revu_.asb_.post_decretdgtv2presidents.pdf

[19] https://www.amf-france.org/sites/institutionnel/files/private/2021-01/doc-2019-17_vf2_ld-ppe.pdf

LE LIVRE BLANC
LA RÉGLEMENTATION GDA & PPE
NIVEAU AUTORITÉS DE CONTRÔLE

La Réglementation dans les domaines du gel des avoirs et des PPE

5. LE NIVEAU DES AUTORITÉS DE CONTRÔLE :

Le cinquième niveau est le niveau des autorités de contrôles. Nous considérons la jurisprudence des autorités de contrôles comme le cinquième niveau de doctrine dans le domaine du LAB. En effet, dans les sanctions prononcées et rendues publiques par l'ACPR, l'AMF, et la CNS (Commission Nationale des Sanctions) se trouvent des énoncés et des explications des règles applicables dans les domaines du Gel des avoirs et des PPE qui s'avèrent extrêmement pratiques.

Nous n'hésitons pas à prendre le raccourci qui consiste à dire qu'être conforme c'est avant tout réussir, sans sanction et remédiation, un contrôle des autorités.

Nous présentons dans la liste suivante les exigences telles que formulées par les autorités à travers les sanctions prononcées, en considérant que le non-respect de ces règles conduira très probablement à des sanctions administratives et à un plan de remédiation qui consiste en lui-même une sanction eu égard aux moyens qu'il devra mobiliser.

Ces exigences concernent à la fois le gel des avoirs et les personnes politiquement exposées :

EXIGENCES CLÉS RELEVÉES DANS LA JURISPRUDENCE

Complétude des relations d'affaires filtrées
Complétude des données des relations d'affaires
Qualité des données des personnes filtrées
Qualité et Complétude des listes de personnes utilisées
Fréquence de mise à jour des listes utilisées
Fréquence de filtrage des relations d'affaires
Algorithmes utilisés pour déterminer la similarité entre les personnes
Délai d'information sur les alertes détectées
Délai de qualification des alertes
Modalité de qualification des alertes
Traçabilité des filtrages réalisés et des alertes traitées

LE POINT DE VUE D'ASTRÉE AVOCATS

LES CONDAMNATIONS POUR MANQUEMENTS AUX OBLIGATIONS LCB-FT SE MULTIPLIENT

Ces dernières années les autorités de nombreux secteurs (ACPR pour l'assurance, AMF pour les marchés financiers…) ont fait de la LCB-FT un thème de contrôle prioritaire. À titre d'illustration l'ACPR a sanctionné 6 établissements en 2023 pour des manquements en LCB-FT.

De manière générale pour le gel des avoirs, les autorités insistent sur la fréquence de filtrage qui doit être quotidienne. Ce filtrage ne doit pas être fait en fonction « exact match », l'outil doit donc prendre en compte les variations orthographiques.

Les autorités sanctionnent souvent une connaissance lacunaire de la clientèle et son impact sur la qualité du filtrage.

Enfin, il est également souvent rappelé que toute personne faisant l'objet d'une mesure de gel des avoird et détectée lors d'un filtrager doit impérativement être déclarée à la Direction Générale du Trésor.

S'agissant des PPE il est rappelé que les mesures de détection doivent porter sur l'ensemble de la clientèle et les bénéficiaires effectifs.

Un point important à retenir ; contrairement au gel des avoirs, l'obligation de filtrer les PPE est une obligation de moyens et non de résultats.

CHAPITRE 3

DÉTECTER UNE PERSONNE SOUS SANCTION OU UNE PPE

Que demande la réglementation lorsqu'il s'agit de détecter une personne sous-sanction ou une PPE ?

Contrairement à certaines idées reçues, la réponse est différente selon qu'il s'agit de la détection des personnes sous sanctions et de la détection des PPE.

Conçu par une équipe de 11 architectes dont Oscar Niemeyer et Le Corbusier, le siège de l'ONU est bâti sur l'East River à New-York. Le projet fut accepté en 1947 et la construction dura jusqu'en 1952. La tour de 39 étages représentée ici abrite le secrétariat.

L'appariement comme méthode pour détecter une personne sous sanctions

Pour les personnes sous sanctions, il faut trouver « qui dans ses relations d'affaires » est présent dans une liste de sanctions. Il s'agit donc de :

rechercher dans une ou plusieurs listes de personnes sous sanction la présence de relations d'affaires
ou
rechercher dans son fichier de relations d'affaires la présence d'une ou de plusieurs personnes qui figurent dans une liste de sanctions. Pour systématiser ses recherches, il faut appliquer une méthode d'appariement qui consiste à unir des paires.

Dans le domaine des personnes sous-sanctions, la paire est constituée d'une part par une personne sous sanction qui figure dans une liste officielle, et d'autre part par une relation d'affaires (clients, payeur, adhérent, prospect, ...).

Et pour chaque paire constituée, il faut déterminer si la personne présente de chaque côté de la paire est la même. Dans ce cas, elle sera qualifiée de « vrai positif ».
Ainsi, toute paire non retenue sera qualifiée de « faux positif » ou « vrai négatif »

Que faut-il faire pour constituer des paires « de personnes » ? La première réponse qui vient à l'esprit est de faire une comparaison exacte des éléments constitutifs de l'identité de la personne, par exemple une comparaison exacte des noms, prénoms et dates de naissance.

MAIS COMPARAISON EXACTE NE SIGNIFIE PAS PERTINENCE POUR PLUSIEURS RAISONS :

- L'exact matching n'est pas accepté par la réglementation[21].
- Des critères orthographiques trop restrictifs dans le paramétrage de l'outil de filtrage ne permettent pas une détection efficace des opérations au profit des personnes ou entités désignées. Les organismes financiers s'assurent donc que leur outil de filtrage ne repose pas sur une fonction de rapprochement de type « exact match ». Ils sont invités à définir un taux de concordance qui permet de détecter les différentes variations orthographiques des éléments d'identification des personnes ou entités désignées en particulier lorsque ceux-ci sont issus de langues ou d'alphabets étrangers.
- Les données d'état civil peuvent être incomplètes ou peu fiables[22]. Les données de personnes sous sanction sont souvent incomplètes et parfois non vérifiables (nous pensons ici aux dates de naissances)
- Des erreurs peuvent intervenir au moment du relevé de l'identité : erreurs typographiques ; erreurs phonétiques, pris en compte de surnoms ou d'alias,
- Des difficultés particulières peuvent apparaitre lorsqu'il est nécessaire de changer d'alphabets l'une des 2 identités de la paire, voire les 2 identités de la paire.

Il faut donc utiliser d'autres méthodes de comparaisons applicables aux noms, prénoms et dates de naissance.
Au-delà du secteur de la criminalité financière, les besoins dans de nombreux secteurs d'activités ont permis de faire émerger de nombreuses techniques pouvant être classées dans **3 familles :**

- **La famille des distances d'édition** : les distances d'édition permettent de comparer deux mots entre eux, ou plus généralement deux séquences de symboles entre elles. Les méthodes les plus connues étant la méthode de Levenshtein et la méthode de Jaro-Winckler.
- **La famille des techniques phonétiques :** l'objectif est que les noms ayant la même prononciation soient codés avec la même chaîne de manière à pouvoir trouver une correspondance entre eux. Les méthodes les plus connues étant la méthode de Soundex et la méthode Métaphone.
- **La famille des techniques de règles :** l'objectif est de s'appuyer sur un référentiel de règles qui permet d'associer des noms et/ou prénoms. Il peut s'agir de dictionnaires pour trouver les diminutifs d'un prénom, ou encore des règles de latinisation ou romanisation permettant de transcrire un mot dans une langue utilisant un alphabet autre vers une écriture latine. Enfin, il peut s'agir d'utiliser des règles prédéfinies (comme ignorer les espaces, la casse, ou les titres).

De nombreuses études ont recherché dans différents contextes, à évaluer ces différentes méthodes et à construire des classements permettant aux utilisateurs de choisir sinon la meilleure méthode, tout au moins la ou les méthodes les plus appropriées.

Retenons dans ces circonstances que les techniques mixtes de « name matching », qui combinent plusieurs approches d'appariement de noms, peuvent être très efficaces dans de nombreuses situations.

Voici quelques raisons pour lesquelles elles sont souvent considérées comme avantageuses :

- **Complémentarité des Techniques :**
Chaque technique d'appariement de noms a ses forces et ses faiblesses. En les combinant, on peut tirer parti des avantages de chacune, ce qui augmente la probabilité de trouver un match correct.
- **Flexibilité et Robustesse :**
Les techniques mixtes offrent une plus grande flexibilité et robustesse, en particulier dans les cas où les données sont imparfaites, incomplètes ou sujettes à des variations.
- **Amélioration de la Précision :**
En utilisant plusieurs méthodes, il est possible de réduire les faux positifs (matches incorrects) et les faux négatifs (matches manqués), améliorant ainsi la précision globale du processus de matching.
- **Adaptabilité :**
Les techniques mixtes peuvent être plus facilement adaptées à des contextes spécifiques, comme des différences linguistiques ou culturelles, qui peuvent affecter la façon dont les noms sont écrits ou prononcés.
- **Traitement de cas complexes :**
Certaines situations de matching de noms peuvent être très complexes (par exemple, des noms très communs ou des noms avec de nombreuses variantes). Les approches mixtes sont souvent plus efficaces pour gérer ces complexités.
- **Utilisation des Avancées Technologiques :**
L'intégration de techniques basées sur l'IA et le machine learning avec des méthodes plus traditionnelles peut profiter des dernières avancées en matière de traitement de données et d'analyse.

En conclusion, le recours à des techniques de « name matching » ou « name screening » est absolument nécessaire pour répondre aux exigences d'identification des personnes sous-sanction.

[21] Considérant 72 - Lignes directrices conjointes de la Direction Générale du Trésor et de l'Autorité de contrôle prudentiel et de résolution sur la mise en œuvre des mesures de gel des avoirs

[22] Selon la banque mondiale environ 850 millions de personnes dans le monde ne disposent pas d'une forme officielle d'identification

Les 3 méthodes complémentaires pour détecter une PPE

Nous distinguons les Personnes Politiquement Exposées des sanctions internationales car il est impossible de construire des listes complètes et tenues à jour de PPE :

●COMPLÉTUDE DES LISTES :
Dans un pays comme la France, les PPE ne sont pas « fichées », en d'autres termes il n'y a pas de listes officielles. Curieusement, il serait de la responsabilité des entreprises assujetties à la lutte contre le blanchiment de construire elles-mêmes ces listes, ou de les acheter à des sociétés spécialisées. Nous ne croyons pas qu'il soit possible de construire des listes exhaustives de PPE en respectant nos libertés individuelles : de quel droit serait-il possible de ficher tous les parents, tous les conjoints, et tous les enfants des PPE de niveau 1 ?

Au niveau international, l'idée même d'être capable de disposer de listes de PPE complètes est une chimère.

●MISE À JOUR DES LISTES :
Il parait encore plus improbable de tenir à jour en permanence des listes de PPE. Qui peut croire que les millions de PPE qui existent dans le monde puissent être fichées de telle manière que tous les mariages, divorces, naissances et décès relatifs à ces personnes puissent être instantanément connus et mis à jour ?

Ces réflexions ont en partie été développées par le GAFI dans sa recommandation sur les PPE. Il y est précisé que pour les PPE, il est nécessaire d'appliquer **3 méthodes complémentaires :**

1. Le questionnaire de connaissance client où il est demandé au client de préciser s'il est PPE ou s'il est proche d'une PPE ou s'il est en relation d'affaire avec une PPE

2. L'identification de PPE à partir de critères d'alertes encore appelés « red flags ». Par exemple en analysant la profession ou encore en croisant la profession et le secteur d'activité du client ou son entreprise

3. En utilisant pour le filtrage des listes de personnes suffisamment qualifiées (listes d'élus,...). Nous revenons ici aux problématiques d'appariements développées pour le filtrage des personnes sous sanctions internationales.

LE LIVRE BLANC
DÉTECTER LES PPE : 3 MÉTHODES

LE POINT DE VUE DE BeCLM

“ COMMENT SONT CONSTITUÉES NOS LISTES PPE ?

La gestion des listes PPE BeCLM est organisée autour de 3 process :
- La R&D
- Le traitement des listes semi-automatisées
- Le traitement des listes non-automatisée

Les 3 process de traitement des listes PPE sont adressés par 4 acteurs différents : un partenaire et 3 services internalisés BeCLM.

1. NOTRE PARTENAIRE ASTRÉE AVOCATS intervient en amont et en aval du traitement des listes :
En amont : veille réglementaire de tous les changements législatifs et réglementaires sur les listes PPE. Analyse de la jurisprudence ACPR lorsqu'elle donne des bonnes pratiques à respecter
En aval, nous demandons à Astrée Avocats d'auditer périodiquement nos listes.

2. LE SERVICE « DATA INTELLIGENCE » BECLM
Il est en charge de toute la gestion de nos contenus.

3. LE SERVICE R&D BeCLM
Il développe les programmes informatiques (Java, Python, IA ...) nécessaires aux traitements des données des PPE :
- des API pour converser en temps réel avec certains sites officiels
- des automates de constructions semi-automatique des listes (par exemple sur les sites des Journaux officiels)
- Des programmes d'extraction de données de certains sites officiels
- Des programmes de nettoyage, translittération et normalisation des données

4. LE SERVICE CONTRÔLE INTERNE
Ce service a pour responsabilité de vérifier en permanence la mise à jour des listes et d'informer nos clients de changements spécifiques notamment en cas d'évolution de la réglementation. ”

Découvrez l'intégralité de nos process listes PPE : *https://www.beclm.com/listes-de-ppe-gratuites-beclm/*

CHAPITRE 4

LES SOLUTIONS LOGICIELLES DE « NAME SCREENING » VUE D'ENSEMBLE

Le « name screening » est un processus crucial pour les personnes assujetties à la réglementation contre le blanchiment d'argent et le financement du terrorisme.

Il permet de filtrer les noms de clients et d'entités avec des listes de surveillance afin d'identifier les risques potentiels de « criminalité financière ».
Diverses solutions logicielles sont disponibles sur le marché pour automatiser ce processus. Revue.

Contruit entre 1984 et 1989, l'immeuble du ministère de l'Économie, des Finances et de l'Industrie a une surface totale de 260 000m2. Un système informatisé de transport du courrier composé de 500 wagonnets y dessert 120 « gares ».

Les caractéristiques clés des solutions logicielles

Les solutions logicielles de « name screening » offrent plusieurs fonctionnalités clés :

1. **Le filtrage automatisé** : Il automatise le processus de vérification des noms contre des listes de sanctions, des listes de surveillance des PEP (Personnes Exposées Politiquement), et des bases de données de réputation.

2. **Les mises à jour en temps réel :** Ces systèmes sont régulièrement mis à jour pour refléter les changements dans les listes de sanctions et autres bases de données pertinentes.

3. **Analyse de données avancée :** Utilisation de l'intelligence artificielle et de l'apprentissage automatique pour améliorer la précision du filtrage et réduire les faux positifs.

4. **Intégration des systèmes via des API :** Capacité à s'intégrer dans les systèmes existants des entreprises pour un flux de travail unifié.

5. **Rapports et traçabilité :** Génération de rapports détaillés pour les audits et preuves de conformité.

Le choix d'une solution logicielle doit se faire non seulement en évaluant ses fonctions clés mais surtout sur la base des cas d'utilisation critiques répertoriés par l'entreprise.

Choix des solutions logicielles : les cas d'utilisation critiques à prendre en compte

Il existe une grande variété de solutions logicielles pour faire du « name screening », des plus simples aux plus sophistiquées, des peu chères aux très onéreuses, des faciles à mettre en œuvre à celles qui nécessitent de véritables projets d'intégration. Ces diverses solutions peuvent être catégorisées comme suit :

- Solution bureautique de type tableur
- CRM avec fonction intégrée de « name screening »
- Solution métier (assurance, immobilier, comptabilité, ...) avec fonction intégrée de « name screening »
- Site web officiel (DGT, OFAC, ...)
- Plateforme API
- Développement « maison » c'est-à-dire développement spécifique
- Progiciel spécialisé (mode SaaS ou On Premise)

POUR FAIRE UN CHOIX, IL FAUT SE FOCALISER SUR LES CAS D'UTILISATION CRITIQUES EN REGARD DE L'ACTIVITÉ EXERCÉE.

LE VOLUME DES DONNÉES À FILTRER

Certaines solutions sont incapables de traiter des volumes importants de personnes à filtrer. La volumétrie critique est celle du portefeuille de relations d'affaires. Selon que l'unité de comptage des relations d'affaires en portefeuille est la centaine, le millier, ou le million, certaines solutions logicielles peuvent s'avérer totalement inopérantes.

La réglementation impose de filtrer l'intégralité de son portefeuille de relations d'affaires à chaque fois qu'une liste de sanctions imposée par la réglementation est modifiée. Les autorités de contrôles sanctionnent les entreprises qui ne filtrent pas quotidiennement l'intégralité de leur portefeuille.

Le temps de traitement du filtrage va dépendre bien entendu de l'algorithme utilisé pour le « name screening » mais aussi du volume de relations d'affaires (Va) à filtrer, et du nombre de personnes présentes dans les listes (Np) , sanctions et PPE. Si on considère, un traitement non optimisé, il faudra effectuer Va x Np calculs.

Pour un volume de 10.000 relations d'affaires, et une liste de 10.000 personnes, il faut effectuer 100 millions de calculs. Le bon « logiciel » est donc le logiciel dont la capacité de calcul est adaptée au volume à la fois de relations d'affaires et des listes de sanctions et PPE utilisées.

Mais au strict traitement de filtrage, il faut ajouter 2 traitements connexes sans lesquels, un filtrage adéquat ne peut se faire :

- **Le transfert du portefeuille de relations d'affaires** : s'il est facile de transférer quelques k octets de données, il est beaucoup plus délicat de transférer des giga octets, car le transfert comprend a minima les opérations d'extractions de la base de données source, de communication des fichiers, et d'intégration dans la base de données cible. Ces opérations sont critiques car sur des volumes importants de données, l'extraction devra être faite sur des plages horaires qui ne viennent pas perturber les autres traitements, et les utilisateurs de la solution informatique qui est la source des données.

- **La piste d'audit** : nous verrons plus loin que la conformité d'un traitement de filtrage repose aussi sur la qualité de sa piste d'audit, or la construction d'une piste d'audit de qualité nécessite une opération d'écriture dans une base de données.
Dans notre exemple précédent avec 10.000 relations d'affaires et une liste globale de 10.000 personnes, il faut aussi insérer en base 100 millions de pistes d'audit.

LE POINT DE VUE DE BeCLM

LE SYNDROME DE LA FERRARI AVEC UN MOTEUR DE 2CV

Avec un moteur de 2CV, une Ferrari ne serait qu'une splendide carrosserie se traînant sur les routes.
De la même manière, une application de filtrage, si bien conçue soit-elle, qui ne reposerait pas sur une infrastructure informatique puissante et intelligente, calera à un moment sur une quantité de données trop importante à traiter.

BeCLM a choisi d'investir dans une architecture Kubernetes pour offrir à ses clients :

- une puissance de filtrage qui s'adapte en temps réel au volume de données à traiter
- zéro interruption de service en cas de faille du système

POURQUOI KUBERNETES EST L'ARCHITECTURE PARFAITE POUR UNE SOLUTION CONFORMITE PERFORMANTE ?

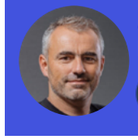
Kubernetes fonctionne grâce à un système de « pods » à la fois indépendants et reliés les uns aux autres. Si un pod tombe en panne, un autre prend le relais jusqu'à son redémarrage. Le traitement des données n'est jamais interrompu, pas même lors du déploiement de nouvelles versions.

Ainsi, avant qu'un pod arrive à saturation de sa capacité de calcul, un deuxième, un troisième, autant que nécessaire, s'activent automatiquement. Le système est à la fois économe en énergie (seule la puissance nécessaire est mobilisée) et ultra-réactif : 500 millisecondes de temps de réaction maximum garanti. Aujourd'hui, le calcul est réalisé EN PARALLELE sur plusieurs ressources, ce qui a permis de diminuer encore le temps de traitement.

Kubernetes permet également d'isoler chaque calcul de chacun de nos clients sur une ressource dédiée. Vos données sont silotées, en sécurité.

Le système choisi par BeCLM assure donc une haute disponibilité dont nos clients sont les premiers bénéficiaires.

Carrosserie et moteur sont à l'avenant.



Etienne Blanchet
D.G. de BeCLM

LES FONCTIONS DE RECALCUL DES MATCHS

Une fonction de recalcul est une fonction qui, comme dans Excel, permet de réexécuter à la demande, ou de manière planifiée, une série de calculs sur certaines données.

Dans les logiciels de « name screening », cette fonction essentielle évite de transférer inutilement l'intégralité du portefeuille à des fins de filtrage. Elle permet aussi de relancer plus facilement les traitements de filtrage en cours de tests, ou de modification du paramétrage, ou encore lorsqu'une liste est modifiée plusieurs fois dans la journée.

La performance d'une fonction de recalcul va elle aussi dépendre du volume des relations d'affaires à filtrer. Mais le volume à prendre en compte en compte est fonction de l'infrastructure matérielle utilisée pour héberger le logiciel de filtrage.

Avec une solution SaaS ou l'infrastructure est généralement mutualisée entre de nombreuses sociétés clientes de l'éditeur, les recalculs peuvent générer des files d'attente, voire le blocage de certains traitements à certaines heures.

Ces problèmes sur les solutions SaaS sont évidemment prégnants lorsque l'éditeur a un positionnement « low cost » qui implique un sous-investissement dans l'infrastructure mise à disposition de ses clients. Il en est de

même avec les solutions métier qui supportent des fonctions de filtrage : Ces traitements de filtrage peuvent venir concurrencer les traitements métier de l'application.

Dans certains cas, il est aussi possible qu'un traitement de filtrage sur un portefeuille ne soit pas terminé avant l'apparition d'une mise à jour de liste officielle. Un peu comme un flash météo qui donnerait le temps de la veille.

L'ORCHESTRATION DES MODES OPÉRATOIRES DE FILTRAGE

La réglementation impose un filtrage dans les situations suivantes :

- Au moment de l'entrée en relation avec une personne physique ou morale, dès lors que sa qualité est visée par la réglementation
- A chaque opération susceptible de modifier le patrimoine de la personne,
- A chaque modification des données de la personne, et plus particulièrement des données permettant d'identifier la personne, et qui sont utilisées par le traitement de filtrage et pour la qualification des alertes
- A chaque nouvelle version d'une liste, sanction ou PPE.

Pour opérer un filtrage, il faut donc disposer d'une solution agile qui doit être compatible avec les exigences de l'activité commerciales, ou des niveaux de services de l'entreprise, et en l'espèce :

- Ne pas bloquer les affaires, ce qui peut être le cas par exemple pour une opération de souscription sur un site internet,
- Ne pas ajouter trop de charge administrative, par exemple pour un chargé d'agence dans une agence,
- Ne pas entrainer trop d'interactions avec d'autres acteurs dans l'entreprise, lorsque par exemple il faut analyser une alerte consécutive à un filtrage.

Dans ces circonstances lorsque la solution est lourde ou contraignante, certaines entreprises préfèrent arbitrer en faveur de l'activité commerciale ou du respect des niveaux de services au détriment du respect de la réglementation.

Le niveau d'agilité de la solution va reposer essentiellement sur la possibilité d'orchestrer différents modes opératoires de filtrage via :

- La saisie ou le filtrage manuel
  - Une relation d'affaire occasionnelle
  - Une entreprise qui demande un devis pour un contrat d'assurance
  - …
- L'import manuel d'un fichier
  - La liste des salariés une fois par mois
  - Des personnes en demande d'affiliation
  - ….
- Le transfert automatisé de fichiers
  - Le portefeuille de relation d'affaires
  - Les sinistres quotidiens à régler
  - …
- Des API
  - Une personne qui souscrit à un contrat sur internet
  - Une personne qui fait une opération de paiement avec une carte bancaire
  - …

LE LIVRE BLANC
CHOIX D'UNE SOLUTION
LES CAS CRITIQUES

LE POINT DE VUE DE BeCLM

LES NOTIONS DE FLUX ET DE SOURCES

Les entreprises ont des sources de données multiples qu'il faut être capable de traiter distinctement. Toutes les personnes qui doivent faire l'objet d'un filtrage ne doivent pas l'être dans les mêmes conditions.

Prenons l'exemple des personnes physiques et des personnes morales. Si elles ne sont pas correctement identifiées, en tant que telles, dans leurs sources de données, il y a un risque de filtrer des personnes physiques avec des personnes morales présentes dans des listes de sanctions par exemple, ou encore de filtrer en tant que personnes politiquement exposées des personnes morales ! En outre la configuration de l'algorithme de filtrage ne sera pas le même, car dans un cas il y a des dates de naissance et dans l'autre pas.

Il est donc indispensable de pouvoir différencier les sources de données afin qu'elle soient configurées différemment dans des « flux » distincts.

UN SYSTÈME AVANCÉ DE CONFIGURATION DES TECHNIQUES D'APPARIEMENT

Comme nous l'avons présenté précédemment, les techniques d'appariement sont consubstantielles aux solutions de « name screening ». Lorsqu'on étudie l'état de l'art de ces techniques, il ressort que le point clé est la capacité de configuration des différentes techniques, en d'autres termes les possibilités d'adaptation à la diversité et à la qualité des données « filtrées ». En toutes circonstances et quels que soient la taille de l'entreprise et son secteur d'activité, il faut que le système de configuration permette de :

- Normaliser toutes les données utilisées pour l'analyse de similarité : suppression des caractères spéciaux, transformation de la casse, …
- Mesurer la similarité entre les termes de l'identité en mixant plusieurs méthodes : méthodes de distances d'édition et méthodes phonétiques particulièrement importantes quand l'acquisition des données des relations d'affaires s'effectue par le canal téléphonique
- Scorer les termes d'une identité en affectant des poids par exemple au nom, au prénom et à la date de naissance
- Attribuer des seuils de détection pour définir dans quelles conditions une « paire » est considérée comme une alerte à traiter.

LE POINT DE VUE DE BeCLM

COMPARONS LES 2 IDENTITÉS « VOVA PUTIN » ET « VLADIMIR POUTINE »

Sous l'angle phonétique (par exemple par Métaphone) il y a une similarité faible, et sous l'angle orthographique la distance de Levenshtein entre les 2 identités est de 9 opérations. Par conséquent la similarité est nulle. En revanche avec un algorithme plus sophistiqué, on va trouver que «Vova» est une diminution affectueuse de «Vladimir» en russe.

Simplifions et comparons les 2 noms « Putin » et « Poutine ».
Dans ce cas, les 2 algorithmes utilisés précédemment donnent tous les 2 une forte similarité : un même phonème (PTN) pour Métaphone et une distance de 3 pour Levenshtein.
Reprenons une comparaison simple de 2 noms « Cocteau » et « Kocto ».

Dans ce cas Levensthein nous dit que les 2 noms ne sont pas similaires (distance de 4) mais Métaphone nous dit que les 2 noms sont fortement similaires (même phonème KKT).

DES LISTES DE PERSONNES ACCESSIBLES EN TEMPS RÉEL

Les listes de sanctions sont en accès libres sur les sites officiels des autorités de chaque pays via des API où en simple téléchargement

ON PRIVILÉGIERA DONC LES SOLUTIONS DE NAME SCREENING OFFRANT UN ACCÈS EN TEMPS RÉELS À CES LISTES, ET QUI NE LES FACTURENT PAS.

Le choix de listes doit être multiple et ne pas se limiter, par exemple, à la seule liste nationale consolidée, pour tenir compte notamment des délais de mises à jour des sanctions décidées par l'ONU ou l'UE, et intégrer via des listes spécifiques, l'ensemble des pays de résidence des relations d'affaires.

Pour les listes de PPE, les mêmes questions se posent. Y accéder est néanmoins moins aisé que pour les listes de sanctions car il faut généralement pour un seul pays accéder à plusieurs sites officiels pour construire une liste nationale complète.

Certains éditeurs font payer ce service en vendant leurs listes ou en achetant eux-mêmes des listes à des « data brokers ». Sur les listes de PPE, il faut aussi obtenir les données des PPE des niveaux 2 et 3 (parents, conjoints, enfants, relation d'affaires) qui relèvent en principe de la sphère privée réglementée par RGPD, à moins qu'elles soient directement accessibles sur des sites publics. Une attention particulière doit donc être portée au contenu de ces listes, et aux modes d'acquisition des données qui y figurent.

UNE CONFIGURATION QUI S'ADAPTE À L'ORGANISATION

Dans les groupes de sociétés avec de multiples filiales ou participations, il est essentiel de pouvoir compartimenter de manière étanche les données de chaque société.

Dans les structures décentralisées, les personnes en charge du traitement des alertes doivent pouvoir accéder aux seules relations d'affaires qui sont dans leur périmètre de gestion.

Dans les structures centralisées, le traitement des alertes doit pouvoir se faire selon un workflow compatible avec l'organisation du service conformité.

UNE CONFIGURATION CAPABLE DE TRAITER DES SOURCES DE DONNÉES MULTIPLES

Il est rarissime que l'origine des données à filtrer soit unique. Elles peuvent être réparties dans de multiples systèmes d'informations : CRM, logiciels métiers, système RH, tableaux excel ...

Dès lors, il faut comprendre les outils et services mis à disposition par l'éditeur pour récolter toutes les données du « stock » et des « opérations » associées à ces différentes sources de données.

En conséquence, sauf dans le cas très spécifique ou les utilisateurs effectuent un « filtrage manuel », dans tous les autres cas l'entreprise qui souhaite mettre en place une solution de « name screening » devra disposer de compétences informatiques disponibles pour « traiter » les différentes sources de données.

LE LIVRE BLANC
CHOIX D'UNE SOLUTION
LES CAS CRITIQUES

UNE INFRASTRUCTURE CONFORME À LA POLITIQUE DE SÉCURITÉ DE L'ENTREPRISE

La question de la politique de sécurité est au centre des préoccupations des DSI, d'autant plus lorsque la solution de « name screening » est mise à disposition en mode SaaS.

Notons que dans un mode SaaS mutualisé entre de nombreuses entreprises, les solutions pour répondre aux exigences de sécurité sont communes à toutes les entreprises, et qu'il est difficile de répondre aux spécificités de chacune d'elles.

La possibilité de mettre en place un SaaS privé propre à une entreprise peut alors faciliter l'adéquation des services de l'éditeur avec les exigences et la stratégie de sécurité de l'entreprise cliente.

LE POINT DE VUE DE BeCLM

« SAAS PRIVÉ OU MUTUALISÉ, UNE QUESTION STRATÉGIQUE

Le choix entre SaaS mutualisé et SaaS privé dépend des besoins spécifiques de l'entreprise en matière de personnalisation, de sécurité, de performance et de coûts.

UN SAAS MUTUALISÉ PERMET :

- Un coût d'infrastructure réduit puisqu'il est généralement partagé entre plusieurs sociétés
- La simplification de la maintenance et du déploiement de nouvelles versions car pris en charge comme un service global

MAIS IMPLIQUE AUSSI :

- Des questions de confidentialité des données partagées entre toutes les entreprises.
- Une potentielle surutilisation liée au partage des ressources qui peut affecter les performances pour tous les utilisateurs.

LE SAAS PRIVÉ PERMET :

- Un contrôle total sur les données sans risque de perméabilité entre entreprises
- Une adaptabilité de la sécurité pour répondre à des besoins spécifiques.
- Des performances moins complexes à maîtriser sur des ressources dédiées

MAIS IMPLIQUE AUSSI :

- des coûts plus élevés avec des infrastructures dédiées et des ressources supplémentaires.
- une complexité de gestion accrue pour la maintenance et les mises à jour.

Beclm a choisi de concevoir et de développer sa solution pour permettre sa mise en œuvre en SaaS mutualisé, en prenant en compte les contraintes liés à ce mode de déploiement (performance, sécurité) pour offrir à ses clients l'agilité sur les mises à jours (évolutivité de la solution) et l'optimisation du coût d'infrastructure en particulier pour les traitements à haute fréquence et grand volume.

Ce choix SaaS privé / SaaS mutualisé est une décision stratégique qui implique l'évaluation du rapport risque/coût.

La solution BeCLM est évidemment déployable en mode Saas privé avec un niveau de service équivalent et les bénéfices d'une solution sur-mesure.

Etienne Blanchet
D.G. de BeCLM

LE MONITORING DES TRAITEMENTS DE FILTRAGE

Les solutions de name screening ne sont pas de simples bases de données « passives » où les utilisateurs effectuent des recherches de personnes concordantes.

Ces solutions sont en activité quasi permanente avec des traitements temps réels et différés associés aux différentes exigences de filtrage, portefeuilles et opérations. La disponibilité et le bon fonctionnement d'une solution de name screening est déterminante pour assurer la conformité réglementaire d'une société.

Il suffit de quelques dysfonctionnements pour que la conformité soit éprouvée :

- Non mise à jour d'une version de listes de sanctions
- Transfert échoué d'un fichier
- API hors service
- …

Il est donc essentiel de mettre en œuvre avec l'éditeur des SLA permettant de contrôler le bon fonctionnement du système.

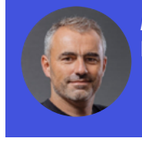
LE POINT DE VUE DE BeCLM

« C'EST COMME SURVEILLER LES FONCTIONS VITALES D'UN ATHLÈTE DE HAUT NIVEAU.

Avec la plateforme de surveillance Grafana, BeCLM monitore en permanence les temps de réponse de l'application, des API, la puissance utilisée et celle qui est disponible.

En résumé : le bon fonctionnement global du système.

Les éventuelles anomalies sont immédiatement repérées et traitées par notre équipe support composée de 5 personnes. Ces informaticiens et techniciens sous astreinte peuvent intervenir jour et nuit, semaine et week-end. Vos données et votre accès à nos solutions sont l'objet de toute notre attention. »



Etienne Blanchet
D.G. de BeCLM

DES SERVICES AUX UTILISATEURS

En première approche l'utilisateur d'une solution de « name screening » va le plus souvent considérer que les cas d'usage sont assez triviaux. Comparer des personnes ne semble pas en effet très compliqué. Mais à l'usage de nombreuses questions et difficultés apparaissent :

- Fonctionnement des algorithmes de matching : pourquoi telle personne apparait avec tel score ? pourquoi telle autre n'a pas été détectée ?
- Nombre de faux positifs à traiter : à quel niveau faut-il paramétrer le seuil de détection ? Pourquoi toutes les sociétés qui comportent le même mot « holding », « corporate » ressortent-elles en anomalies ? …
- Différences entre les listes : pourquoi une même personne apparait sous différentes orthographes dans les listes ONU, FR, IU, OFAC, …
- Pourquoi ai-je une alerte sur une personne alors que mon partenaire ne l'a pas détectée ?
- …

Parce que les exigences réglementaires sont fortes pour les utilisateurs, l'éditeur doit proposer un service de qualité et engagé qui va bien au-delà du simple dépannage ou guidage dans l'application.

LE LIVRE BLANC
CHOIX D'UNE SOLUTION
LES CAS CRITIQUES

LE POINT DE VUE DE BeCLM

« NOS SERVICES AUX UTILISATEURS

Au nombre de 7, nos services aux utlisateurs répondent à l'ensemble des besoins des entreprises assujetties :

1) **L'infrastructure informatique nécessaire au traitement de la big data.**
2) **La technologie « Double run » pour réduire le taux de faux positifs**
3) **L'IA pour vous aider à qualifier et documenter vos alertes en optimisant leur temps de traitement.**
4) **Le niveau de sécurité de votre choix**
5) **Le monitoring permanent des données et de la solution**
6) **La piste d'audit absolue pour répondre à toutes les demandes des autorités sans sacrifier la performance**
7) **L'assistance au quotidien et en cas de contrôle**

Retrouvez les services BeCLM en détail sur *www.beclm.com* »

L'URGENCE DE MISE EN ŒUVRE DE LA SOLUTION

Comme pour tout projet informatique, se poser les bonnes questions sur la mise en œuvre de la solution est primordial.

Lorsqu'il s'agit de se mettre rapidement en conformité ou de remédier dans le cadre d'un audit ou d'un contrôle des autorités, le temps de mise en œuvre de la solution peut s'avérer critique.

LE RADAR DES SOLUTIONS

Solution bureautique de type tableur

Solution à oublier car un système de feuilles de calculs, même sophistiqué, ne peut pas répondre aux besoins critiques.

CRM avec fonction intégrée de « name screening »

Ces solutions peuvent paraître attractives dans un premier temps car a priori les relations d'affaires résident dans le CRM (il faudra néanmoins trouver des solutions pour filtrer d'autres sources de données comme les salariés et les partenaires commerciaux) et elles disposent souvent d'une bibliothèque d'algorithmes de matching.

Toutefois ce type de solutions présente quelques inconvénients majeurs : l'accès aux listes de personnes, listes de sanctions et PPE, la capacité à traiter des volumes importants, notamment lorsque les utilisateurs sont connectés, fonctionnalités basiques pour traiter les alertes.

Solution métier (assurance, immobilier, comptabilité, …) avec fonction intégrée de « name screening »

Elles sont comparables aux solutions CRM mais avec un avantage en moins : elles ne disposent pas de bibliothèques d'algorithmes de matching.

Sites web officiels (DGT, OFAC, …)

Pour des besoins simples de filtrage manuel, ces solutions « officielles » sont pertinentes et en plus elles ont l'avantage d'être gratuites. En revanche, elles ne traitent que les sanctions internationales.

Plateformes d'API

Ces solutions sont à étudier dès lors qu'il existe au moins une API pour supporter chaque cas d'utilisation critique. Il reste à voir sur combien d'applications les API seront déployées. Lorsque les API sont déployées sur plusieurs applications, la gestion de la piste d'audit est plus complexe. Enfin, il faut étudier les conditions de filtrage de l'intégralité du portefeuille. Sur ce point, les limites techniques sont nombreuses.

Développement « maison » c'est-à-dire développement spécifique

Le choix du développement spécifique est avant tout une question de poli-

tique informatique.

Lorsque ce choix est effectué pour des raisons budgétaires, en considérant que le budget du développement « maison » sera inférieur aux coûts des licences et d'intégration d'une solution progicielle, il y a toujours le risque de complétude des fonctionnalités et de qualité de la solution finale.

Enfin, les autorités de contrôles ne semblent pas apprécier ce type de solution.

Progiciels spécialisés (mode SaaS ou On Premise)

Hormis les contextes organisationnels et fonctionnels très simples, le choix d'un progiciel spécialisé va s'imposer. Les éditeurs n'offrent bien entendu pas les mêmes fonctionnalités et les mêmes niveaux de services.

Nous pensons qu'il existe deux familles d'éditeurs, selon qu'ils ont ou non la capacité à adresser des fonctionnalités que nous qualifierons de « Hype » ,c'est-à-dire des fonctionnalités à la pointe de la technologie et/ou à la pointe des services aux utilisateurs.

Sur les 15 cas d'utilisation critiques précédemment présentés nous en retenons 6 qualifiés de « Hype », ils sont recensés dans le tableau ci-contre :

CAS D'UTILISATIONS CRITIQUES	FONCTIONS BANALISÉES	FONCTIONS « HYPE »
Le volume des données à filtrer		Le traitement de gros volumes n'est possible qu'avec un nombre très limité d'éditeurs.
Les fonctions de recalcul des matchs	X	
L'orchestration des modes opératoires de filtrage	X	
Un système avancé de configuration des techniques d'appariement	X	
Des listes de personnes accessibles en temps réel	X	
Une configuration qui s'adapte à l'organisation	X	
Une configuration capable de traiter des sources de données multiples	X	
Une infrastructure conforme à la politique de sécurité de l'entreprise		Tous les éditeurs ne proposent pas à la fois le « On premise », le « Saas mutualisé » et le « SaaS privé »
Un système de notification des alertes en temps réel	X	
Un traitement efficace et précis des alertes		Certains éditeurs ont développé des fonctionnalités avancées d'aide à la qualification et à la documentation des alertes
Une piste d'audit adaptée aux obligations de résultats		Les éditeurs communiquent rarement sur ce sujet car c'est une exigence qui est souvent négligée au profit de la performance. Ainsi, que vaut la vitesse d'une API si celle-ci ne traite pas la piste d'audit ?
Un reporting outillé	X	
Le monitoring des traitements de filtrage		Indispensable pour des solutions sur lesquelles pèsent des obligations de résultat
Des services aux utilisateurs		Indispensable pour des solutions aux fonctionnalités complexes
L'urgence de mise en œuvre de la solution	X	

CHAPITRE 5

TECHNOLOGIES AVANCÉES & NAME SCREENING

Le « name screening » repose sur une gamme de technologies avancées. Ces technologies ne se limitent pas à automatiser les processus existants, elles transforment activement la manière dont les institutions financières abordent la détection et la prévention de la criminalité financière.

Intelligence Artificielle (IA) et Apprentissage Automatique (Machine Learning)

L'IA pour le traitement des alertes.

L'intelligence artificielle et l'apprentissage automatique sont au premier plan dans l'innovation du « name screening ». Ces technologies permettent aux systèmes de filtrage de s'adapter et d'apprendre à partir des données, améliorant ainsi leur précision au fil du temps :

- Détection des Modèles : L'IA identifie des modèles complexes et des relations dans les données, ce qui est particulièrement utile pour reconnaître des activités suspectes.

- Réduction des Faux Positifs : L'apprentissage automatique affine les algorithmes pour distinguer efficacement les vraies menaces et les fausses alertes.

Sur ces utilisations de l'IA appliquées au « name screening », il faut toutefois émettre quelques réserves concernant le niveau d'appropriation des utilisateurs : lorsque l'évaluation des similarités entre les personnes est « déléguée » à un moteur d'IA, avec comme objectif de réduire les « faux positifs », l'utilisateur peut perdre la maitrise des alertes générées par le système.

Ce phénomène de perte de la maîtrise du système est bien connu dans d'autres domaines d'application de l'IA. Nous ne citerons que les logisticiens dont certains ont préféré limiter les usages de l'IA, car ils perdaient le contrôle des décisions opérationnelles (transport, stockage, …) et ne savaient pas comment réagir lorsque l'IA prenait des décisions qui leurs paraissaient irrationnelles.

En revanche, nous pensons que l'IA peut apporter beaucoup de valeur pour aider les utilisateurs à qualifier les alertes et à les documenter. Dans ce contexte d'utilisation bien précis, l'IA est au service de la productivité des utilisateurs.

LE LIVRE BLANC
TECHNOLOGIES AVANCÉES & NAME SCREENING

LE POINT DE VUE DE BeCLM

> **LA PREMIÈRE APPLICATION DE L'IA QUI VIENT À L'ESPRIT**

est son utilisation pour les traitements de filtrage en visant le double objectif de détection systématique des « vrais positifs » et de réduction des « faux positifs ».

Mais lorsque l'évaluation des similarités entre les personnes est « déléguée » à un moteur d'IA, l'utilisateur risque de perdre la maitrise des alertes générées par le système. Ce phénomène de perte de la maîtrise du système est bien connu dans d'autres domaines d'application de l'IA. Nous ne citerons que celui de la logistique où certains logisticiens ont préféré limiter les usages de l'IA, car ils perdaient le contrôle des décisions opérationnelles (transport, stockage, approvisionnements …), et ne savaient pas comment réagir lorsque l'IA prenait des décisions qui leurs paraissaient « étonnantes ».

Dans le domaine de la lutte contre le blanchiment, l'utilisateur est censé Se poser les mêmes questions : il faut se projeter dans le discours à tenir face aux autorités de contrôle lorsqu'elles poseront la question clé : « pourquoi vos filtrages n'ont pas déclenché des alertes sur telles personnes ? ». En outre, il faut aussi s'interroger sur la piste d'audit, et les traces « compréhensibles » qu'elle va laisser pour être en mesure de prouver que telle personne a été filtrée à tel moment, avec tels résultats, dans telle configuration.

POUR TOUTES CES RAISONS, BECLM A FAIT LE CHOIX DE CIRCONSCRIRE LE DOMAINE D'APPLICATION DE L'IA À L'AIDE À LA QUALIFICATION DES ALERTES.

C'est une activité où l'IA permet d'assister les utilisateurs pour qualifier les « faux positifs à travers les questions élémentaires sur les similarités entre des noms ou des prénoms. L'IA permet parallèlement de documenter efficacement les décisions qui sont prises au moment de la qualification de chaque alerte.

Dans le système BeCLM, l'IA permet donc complémenter le PCR™ afin que chaque alerte soit documentée à la fois sur son mode de calcul (Dossier PCR) et sur sa qualification (Dossier IA).

Jean-Marc Lafin
Président de BeCLM

Big Data et Analytics

Les solutions de «name screening» doivent traiter et analyser d'énormes volumes de données pour identifier les risques potentiels. Le Big Data et les technologies analytiques jouent un rôle clé dans la gestion de ces données. Le big data est souvent caractérisé par 3 V :

1. **VOLUME** : Se réfère à la quantité massive de données à exploiter.

- Dans le domaine du name screening, il s'agit essentiellement de la taille du portefeuille de relation d'affaires. Pour certaines sociétés dans le domaine de la banque et de l'assurance, ces portefeuilles peuvent comprendre plusieurs millions voire dizaines de millions de personnes.
- Sont employés dans ce cadre des technologies comme les bases de données NoSQL ou MongoDB, et encore des systèmes de stockage distribué comme Hadoop HDFS.

2. **VITESSE** : Désigne la rapidité avec laquelle ces données sont produites, collectées et traitées.

- Dans le domaine du name screening, l'enjeu est de filtrer le plus rapidement le portefeuille d'affaires et de garder une piste d'audit pour chaque match. Nous pouvons aussi trouver une application pratique au big data lors de la recherche parmi des milliards de documents des pistes d'audit de telle ou telle personne
- Sont employés dans ce cadre des technologies en temps réel comme Apache Kafka et Apache Storm3.

3. **VARIÉTÉ** : Indique la diversité des types de données (structurées, non structurées, semi-structurées) provenant de différentes sources.

- Dans le domaine du « name screening », la diversité des données est une caractéristique qui s'applique essentiellement aux contenus des listes de personnes et en particulier aux listes de personnes sous sanctions.
- Sont employés dans ce cadre des technologies comme ElasticSearch pour la recherche et l'analyse de données textuelles variées, ou des outils d'intégration de données comme Talend pour traiter et transformer différents formats de données.

LE LIVRE BLANC
TECHNOLOGIES AVANCÉES & NAME SCREENING

LE POINT DE VUE DE BeCLM

> **SÉPARER ARCHITECTURE ET PERFORMANCES EST UNE ERREUR**

Les nouvelles technologies ainsi que les infrastructures cloud modernes doivent se mettre au service des exigences fonctionnelles des solutions logicielles. L'architecture ne doit pas être un empilement de composants sans lien avec les performances qui doivent être mesurées et sans cesse améliorées.

L'ARCHITECTURE DE LA SOLUTION BECLM A ÉTÉ CONÇUE EN S'APPUYANT SUR UNE VISION À LONG TERME DES ENJEUX DE FILTRAGE / CONTRÔLE DES DONNÉES :

- Les données qui sont à la base des analyses, données de plus en plus riches, données destructurées, et données qui doivent être mises à jour de plus en plus régulièrement
- Les capacités de traitement et de calcul qui doivent suivre l'augmentation des besoins, en particulier le contrôle permanent
- La traçabilité qui est un enjeu de stockage et d'analyse

La réponse est une articulation entre une architecture logicielle, des algorithmes et une utilisation des infrastructures cloud :

- Architecture hexagonale fortement orientée asynchrone pour permettre la dissociation des traitements, des interfaces utilisateurs et des besoins temps réel. Une architecture également ouverte pour permettre l'intégration par API des données clients et référentiel
- Des algorithmes complexes pour adresser les problématiques de traitement en parallèle
- Une infrastructure cloud reposant sur une adaptabilité aux besoins, avec augmentation des capacités sur les périodes de forte charge

Notre travail constiste à améliorer constamment ces paramètres en faisant intervenir des compétences en architecture, en développement et en devops qui permettent aujourd'hui de garantir :

- une mise à jour en temps réel des listes de contrôle
- une capacité de traitement de plus de 20 millions de personnes en 24h par société
- une conservation des pistes d'audit suivant un principe innovant de PCR alliant aliénation et faible empreinte de stockage.

Etienne Blanchet
D.G. de BeCLM

La technologie Blockchain

La technologie blockchain est un système de registre distribué qui permet de stocker des données de manière sécurisée, transparente et immuable.

Les informations sont enregistrées en blocs liés entre eux et sécurisés via la cryptographie, rendant les données difficiles à modifier ou à falsifier. Principalement connue pour son utilisation dans les cryptomonnaies comme le Bitcoin, la blockchain trouve également des applications dans divers secteurs, tels que la finance, la logistique, et la gestion des identités, en offrant une traçabilité et une fiabilité accrues des informations.

Dans le domaine du name screening, plusieurs applications sont possibles : Première utilisation : le stockage des pistes d'audit. Toutefois, compte tenu du volume très important des pistes à enregistrer, le coût d'une telle solution doit être pris en compte par l'entreprise souhaitant pondérer son budget KYC.

Deuxième utilisation : le « block chaînage » de certains éléments de la configuration ou encore des listes de personnes utilisées pour les filtrages. Là encore, le coût doit être pris en compte.

La forme elliptique de l'atrium du Parlement Européen de Strasbourg fait référence au « Forum ovale » de Jérash (Jordanie), la mieux conservée des cités de la décapole au Proche-Orient antique.

CHAPITRE 6

MEILLEURES PRATIQUES ET ÉTUDES DE CAS

L'efficacité des solutions de «name screening» ne dépend pas seulement de la technologie, mais aussi de la manière dont elles sont implémentées et utilisées.

Ce chapitre explore les meilleures pratiques dans l'utilisation de ces solutions, illustrées par des études de cas concrets.

Meilleures Pratiques dans l'utilisation des solutions de « Name Screening » : Les clés de la Réussite

POUR TIRER LE MEILLEUR PARTI DES SOLUTIONS DE «NAME SCREENING», CERTAINES PRATIQUES SONT ESSENTIELLES :

1. **Faire le choix des listes à utiliser**
2. **Formation continue du personnel (réglementation)**
3. **Procédurer le traitement des alertes (analyses diverses)**
4. **Monitorer ses transferts de données (fichier non envoyés)**
5. **Mettre en place une organisation adaptée au volume d'alertes à traiter**

Les études de cas suivantes illustrent comment différentes sociétés ont réussi à implémenter et optimiser leurs systèmes de « name screening » :

ÉTUDE DE CAS : AGILITÉ

• **Défi** : un établissement financier est confronté aux défaillances répétées de son système de filtrage existant. Il a reçu une injonction administrative d'y remédier le plus rapidement possible.

• **Solution** : sans rien changer au fonctionnement de l'exploitation informatique du client, nous construisons des « ponts » entre les flux des fichiers existants utilisés par l'application défaillante, et BeCLM, où sont paramétrés une dizaine de « flux Gel des avoirs et PPE » correspondant aux sources de données déjà en place. Avec l'assistance de notre partenaire 4SH, nous élaborons un développement spécifique permettant de reprendre l'historique des alertes, afin de minimiser le volume des qualifications manuelles au moment du démarrage de BeCLM en production.

• **Résultats** : en 48H les flux les plus critiques étaient opérationnels dans BeCLM. Une semaine plus tard tous les flux fonctionnaient en production, et l'historique des alertes a été repris dans BeCLM pour minimiser les travaux des gestionnaires.

ÉTUDE DE CAS : PISTE D'AUDIT

• **Défi** : un délégataire de gestion fait l'objet d'un audit d'une compagnie d'assurances qui lui sous-traite la gestion d'une partie de son portefeuille d'affaires.

Les auditeurs cherchent à vérifier la robustesse du système de preuves mis en place dans le cadre des traitements de filtrage « gel des avoirs ». Les preuves de filtrage auditées concernent non seulement des traitements effectués dans le passé sur certaines relations d'affaires du portefeuille à des dates spécifiques, mais aussi sur la justification précise des configurations actives au moment de ces filtrages : seuil de détection, poids des attributs dans les scores … versions de listes de sanctions utilisées.

• **Solution** : pour toutes les demandes, le client a utilisé dans BeCLM la fonction de recherche PCR™ lui permettant d'accéder aux pistes d'audit complètes.

• **Résultats** : satisfaits par la qualité des dossiers de preuves qui leur ont été remis, les auditeurs ont demandé des accès à l'application afin qu'ils puissent à distance opérer leurs contrôles actuels et futurs.

LE LIVRE BLANC
MEILLEURES PRATIQUES & ÉTUDES DE CAS

ÉTUDE DE CAS : SAAS PRIVÉ

• **Défi** : un organisme financier souhaite des engagements stricts sur des niveaux de services, et notamment sur le délai de traitement de ses fichiers qu'il souhaite immédiat dès lors que la réception a été acquitté par nos soins.

• **Solution** : pour s'abstraire du temps de latence qui peut parfois exister sur une solution en SaaS standard au moment de l'exécution de traitements lourds, nous avons déployé la solution sur un SaaS privé.

• **Résultats** : tous les fichiers sont immédiatement intégrés au moment de leurs réception, et grâce au plan de production planifié, nous sommes en mesure d'ajuster au niveau horaire les ressources informatiques allouées, et donc d'optimiser le budget d'hébergement.

ÉTUDE DE CAS : DOCUMENTATION DES ALERTES

• **Défi** : un de nos clients nous explique les difficultés qu'il rencontre concernant la documentation des alertes. Malgré une procédure écrite très détaillée, et les formations dispensées auprès des gestionnaires en charge du traitement des alertes, ces derniers éprouvent des difficultés rédactionnelles au moment de la qualification des dossiers de risques.

• **Solution** : grâce à l'IA générative intégrée dans nos écrans de qualification des alertes, nous avons paramétré des prompts qui suivent scrupuleusement la procédure écrite de l'entreprise.

• **Résultats** : les gestionnaires n'ont plus qu'a contrôler le rapport écrit proposé par l'IA et y apporter éventuellement quelques ajustements.

ÉTUDE DE CAS : LE FILTRAGE DES CLIENTS ATTACHÉS À LA SPHÈRE DE CONFIANCE

• **Défi** : notre client qui distribue et gère des contrats d'assurance vie s'inquiète du délai nécessaire pour traiter certaines alertes générées au moment du filtrage. Il craint que certaines affaires n'aboutissent pas dans le cas où un dossier de souscription est bloqué par une alerte créée par l'API de filtrage BeCLM, intégrée sur son site internet.

• **Solution** : l'étape de vérification des pièces d'identité étant obligatoire dans le domaine de l'assurance vie, nous avons proposé à notre client de mettre en place une solution de type identité numérique pour contrôler et capter les données d'identités des clients.

• **Résultats** : grâce au couplage des solutions d'identité numérique et de filtrage nous avons pu inscrire la majorité des clients dans une sphère de confiance est diminuer par 4 l'effort quotidien de traitement des alertes tout en renforçant la qualité des contrôles.

ÉTUDE DE CAS : DIMINUTION DES FAUX POSITIFS

• **Défi** : une société d'assurance dont le volume de relations d'affaires est très élevé souhaite limiter le temps passé au traitement des alertes et donc des faux positifs.`

• **Solution** : après une analyse détaillée de son portefeuille nous avons pour identifier plusieurs attributs secondaires des clients (nationalité, profession, âge, …) sur lesquels nous pouvions enclencher, dans une « Run 2 », une qualification automatique des alertes après filtrage (« Run 1 »).

• **Résultats** : la solution « double Run » a permis de limiter à 20 minutes le temps de traitement quotidien des alertes d'hébergement.

ÉTUDE DE CAS : LE CONTRÔLE ADMINISTRATIF

- **Défi** : une mutuelle cliente de BeCLM depuis 5 ans fait l'objet d'un contrôle administratif LAB pendant une absence prolongée de son responsable conformité. Le Directeur Général qui assure l'intérim de ce poste clé nous demande de l'assister.
- **Solution** : notre Service Desk s'attache pendant toute la durée du contrôle les services d'un collaborateur d'Astrée Avocats.
- **Résultats** : le contrôle se termine favorablement pour la mutuelle.

ANNEXES

GLOSSAIRE, RÉFÉRENCES LÉGISLATIVES & RÉGLEMANTAIRES

Cette section enrichit le contenu principal du livre blanc, fournissant des détails supplémentaires, des références et des ressources pour une exploration plus approfondie des sujets traités.

glossaire

- **ALERTE D'URGENCE** :

Notification immédiate signalant un risque imminent ou une activité suspecte nécessitant une action immédiate de la part des responsables de la conformité ou de la sécurité.

- **ALERTE DE CONFORMITÉ** :

Notification générée par un système de surveillance ou de filtrage, indiquant qu'une transaction, un nom ou une activité présente un risque potentiel en termes de conformité réglementaire, de sécurité financière ou de lutte contre le blanchiment d'argent.

- **ALERTE PRIORITAIRE** :

Notification signalant un risque élevé ou critique en termes de conformité réglementaire, de sécurité financière ou de lutte contre le blanchiment d'argent, nécessitant une action immédiate ou une enquête approfondie de la part des responsables de la conformité.

- **ALGORITHME DE DOUBLE MÉTAPHONE** :

Une amélioration de l'algorithme de Métaphone permettant de générer deux codes phonétiques pour chaque mot, afin de mieux gérer les noms de famille d'origines diverses et les mots à double sens.

- **ALGORITHME DE MÉTAPHONE** :

Méthode phonétique utilisée pour encoder un mot en une chaîne de caractères représentant sa prononciation phonétique, permettant de rechercher des noms similaires en termes de prononciation malgré des orthographes différentes.

- **ALGORITHMES DE COMPARAISON DE CHAÎNES DE CARACTÈRES** :

Méthodes informatiques utilisées pour mesurer la similitude entre deux chaînes de caractères, en tenant compte des variations telles que les fautes de frappe, les différences d'orthographe, les abréviations et les synonymes.

- **ANALYSE DE SIMILARITÉS** :

Processus informatisé visant à identifier les noms ou les entités qui présentent des similitudes phonétiques, orthogra-

phiques ou linguistiques avec ceux figurant sur les listes de sanctions ou les listes de personnes politiquement exposées (PPE).

- **BÉNÉFICIAIRE EFFECTIF** :

La personne physique qui, en dernière instance, possède, contrôle ou bénéficie de manière significative d'une entité ou d'un compte financier, souvent utilisée pour dissimuler la véritable propriété ou le contrôle d'une entreprise ou d'un actif.

- **BLANCHIMENT D'ARGENT** :

Processus par lequel des fonds provenant d'activités illégales ou criminelles sont intégrés dans le système financier afin de dissimuler leur origine illicite et de les rendre légitimes.

- **CONFORMITÉ KYC (KNOW YOUR CUSTOMER)** :

Processus par lequel les institutions financières et autres entreprises vérifient l'identité, la fiabilité et l'activité économique de leurs clients afin de se conformer aux réglementations anti-blanchiment d'argent et de lutte contre le financement du terrorisme.

- **CONFORMITÉ RÉGLEMENGAIRE** :

Processus par lequel les institutions financières et autres entreprises s'assurent qu'elles respectent toutes les lois, réglementations et normes applicables à leur secteur d'activité, y compris celles liées à la lutte contre le blanchiment d'argent, le financement du terrorisme et les sanctions internationales.

- **ÉVALUATION DES RISQUES** :

Processus d'identification, d'analyse et d'évaluation des risques potentiels auxquels une institution financière ou une entreprise est exposée, notamment en ce qui concerne le blanchiment d'argent, le financement du terrorisme et d'autres activités illicites.

- **FAUX POSITIF** :

Résultat d'une alerte ou d'une détection incorrecte, indiquant à tort qu'une transaction ou un individu présente un risque, alors qu'en réalité, il est légitime et conforme à la réglementation.

- **FINANCEMENT DU TERRORISME :**

Fourniture de fonds ou de ressources financières à des groupes terroristes ou à des individus associés à des activités terroristes, visant à soutenir, promouvoir ou faciliter des actes de terrorisme.

- **FONCTION DE HACHAGE :**

Fourniture de fonds ou de ressources financières à des groupes terroristes ou à des individus associés à des activités terroristes, visant à soutenir, promouvoir ou faciliter des actes de terrorisme.

- **GESTION DES ALERTES :**

Processus de suivi, de traitement et de résolution des alertes générées par un système de surveillance ou de filtrage, impliquant souvent la collaboration entre différents départements tels que la conformité, la sécurité et les opérations.

- **INVESTIGATION D'ALERTE :**

Processus d'examen approfondi des alertes générées par un système de filtrage ou de surveillance, visant à déterminer la légitimité ou la validité des risques détectés et à prendre des mesures appropriées en conséquence.

- **LEVENSHTEIN DISTANCE :**

Une mesure de la différence entre deux séquences de caractères, basée sur le nombre minimum d'opérations nécessaires pour transformer une séquence en une autre (insertions, suppressions ou substitutions de caractères).

- **LISSAGE DES ALERTES :**

Processus de réduction du nombre d'alertes générées par un système de surveillance ou de filtrage, en utilisant des techniques telles que la révision des seuils de détection, l'amélioration des algorithmes de classification ou l'optimisation des paramètres de filtrage.

LE LIVRE BLANC
ANNEXES

- **LISTE DE SURVEILLANCE :**

Liste interne maintenue par une entreprise ou une institution financière, contenant des noms d'individus, d'entités ou de pays présentant un risque potentiel en termes de conformité réglementaire, de sécurité financière ou d'intégrité des transactions.

- **LISTES DE PERSONNES POLITIQUEMENT EXPOSÉES (PPE) :**

Catalogues de personnes qui occupent ou ont occupé des fonctions politiques importantes, ainsi que de leurs proches associés, utilisés pour identifier les bénéficiaires effectifs et évaluer les risques de blanchiment d'argent et de corruption.

- **LISTES DE SANCTIONS :**

Registres officiels émis par des gouvernements, des organisations internationales ou des autorités de régulation, répertoriant les individus, les entités ou les pays faisant l'objet de sanctions économiques, financières ou commerciales.

- **N-GRAMS :**

Technique de traitement du langage naturel consistant à diviser une séquence de caractères en sous-séquences de n caractères consécutifs, permettant de mesurer la similitude entre deux chaînes de caractères en tenant compte de leurs sous-séquences communes.

- **NAME SCREENING :**

Processus de vérification des noms des individus ou des entités par rapport à des listes de sanctions ou des listes de personnes politiquement exposées (PPE) pour des raisons de conformité réglementaire et de lutte contre le blanchiment d'argent et le financement du terrorisme.

- **PERSONNES POLITIQUEMENT EXPOSÉES (PPE) :**

Individus qui occupent ou qui ont occupé des postes politiques importants ou des fonctions publiques de responsabilité, ainsi que leurs proches associés, pouvant présenter un risque accru de corruption ou de blanchiment d'argent.

- **RISQUE DE RÉPUTATION :**

La probabilité qu'une entreprise ou une institution financière subisse des dommages à sa réputation en raison de son implication dans des activités illicites, des violations de la conformité réglementaire ou des erreurs de détection des risques.

- **SANCTIONS INTERNATIONALES :**

Mesures coercitives imposées par un gouvernement ou une organisation internationale à l'encontre d'un pays, d'un groupe ou d'une entité spécifique pour des raisons politiques, économiques, militaires ou sociales.

- **SOUNDEX :**

Algorithme phonétique utilisé pour indexer les noms de famille en fonction de leur prononciation, en les convertissant en une chaîne de caractères numérique, permettant de rechercher des noms similaires en termes de sonorité

- **TAUX DE FAUX POSITIFS :**

Mesure statistique représentant la proportion d'alertes ou de détections incorrectes par rapport au nombre total d'alertes générées par un système de filtrage ou de surveillance, souvent utilisée pour évaluer l'efficacité et la précision du système.

Références récentes législatives et réglementaires

- **LÉGISLATION ET RÉGLEMENTATION FRANÇAISES :**

Code Monétaire et Financier (CMF) :

Loi n° 2019-486 du 22 mai 2019 relative à la croissance et la transformation des entreprises (loi PACTE), notamment ses dispositions concernant la lutte contre le blanchiment d'argent et le

financement du terrorisme. [Legifrance](https://www.legifrance.gouv.fr/loda/id/JORFTEXT000038496102)

Autorité de Contrôle Prudentiel et de Résolution (ACPR)

Circulaire ACPR du 26 décembre 2019 relative à la lutte contre le blanchiment d'argent et le financement du terrorisme, énonçant les lignes directrices et les recommandations pour les établissements soumis à son contrôle. [ACPR](https://acpr.banque-france.fr/sites/default/files/medias/documents/20191218_asr_lcbft.pdf)

Tracfin

Guide des bonnes pratiques de Tracfin pour la détection et la déclaration des opérations suspectes, dernière version mise à jour, disponible sur le site officiel de Tracfin. [Tracfin](https://www.economie.gouv.fr/tracfin/lignes-directrices)

• LÉGISLATION ET RÉGLEMENTATION EUROPÉENNES :

Directive européenne (UE) 2018/843 (5ème directive anti-blanchiment

Directive modifiant la directive (UE) 2015/849 relative à la prévention de l'utilisation du système financier aux fins du blanchiment d'argent ou du financement du terrorisme, publiée en 2018. [Eur-Lex](https://eur-lex.europa.eu/eli/dir/2018/843/oj)

Règlement (UE) 2015/847

Règlement sur les informations accompagnant les transferts de fonds et certaines informations accompagnant les paiements électroniques, toujours en vigueur depuis son adoption en 2015. [Eur-Lex](https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32015R0847)

Autorité Bancaire Européenne (EBA)

Orientations et recommandations de l'EBA sur la lutte contre le blanchiment d'argent, notamment les dernières lignes directrices publiées sur la mise en œuvre de la 5ème directive anti-blanchiment. [EBA](https://eba.europa.eu/regulation-and-policy/anti-money-laundering-and-countering-financing-terrorism)

Groupe d'Action Financière (GAFI)

Recommandations du GAFI (FATF) :

Les dernières recommandations et notes interprétatives du GAFI, y compris les mises à jour apportées par la publication de la 5ème directive anti-blanchiment de l'UE. [FATF-GAFI](https://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html)

Évaluations Mutuelles du GAFI :

Les rapports d'évaluation mutuelle les plus récents des pays membres du GAFI, fournissant des analyses détaillées de leur cadre juridique et réglementaire de lutte contre le blanchiment d'argent. [FATF-GAFI](https://www.fatf-gafi.org/en/countries.html)

Guidelines and Guidance du GAFI :

Les documents d'orientation et les guides techniques du GAFI sur divers aspects de la lutte contre le blanchiment d'argent, régulièrement mis à jour pour refléter les meilleures pratiques et les développements récents. [FATF-GAFI](https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/Ml-tf-risks.html)

LE LIVRE BLANC

LES LOGICIELS DE FILTRAGE « NAME SCREENING »

www.beclm.com
elie.lafin@beclm.com
67 avenue Pierre Grenier - 92100 Boulogne Billancourt
+33 (0)1 46 10 43 82